Q and A on Risk Assessment Part 2

Question 1. What do I do if my small audit client doesn't have any controls?

Answer. Sometimes auditors of LCEs think that their clients have no controls or that their clients' controls can't be effective because there is no segregation of duties. If you represent that your client has no effective controls, you are implying that your client has no effective policies or procedures to prevent or detect errors or frauds. If that were really the case, would you ever be able to do enough auditing to obtain sufficient, appropriate audit evidence to reduce audit risk to an acceptably low level? We think not. The fact is, LCE entities often have simple controls, even though the system may be less formal or need more documentation of the controls to satisfy audit documentation requirements should the auditor want to test the controls. Regardless of an LCE's challenge to have effective controls, you need to understand that LCEs typically will have certain foundational controls that are in place. Hopefully, those controls will include an effective tone at the top (control environment) as well as some control activities such as reconciliations of material accounts, approvals of larger transactions, and various input and cutoff controls. Preventive and detective controls might be present in any of the five components of internal control – not solely in the control activities component. For example, a policy that promotes ethical behavior is a control within the control environment. This nuance has confused some practitioners who previously thought that a control was different from a policy or that controls only existed in the control activities component.

Question 2. Am I ever required to test controls?

Answer. It depends on what you mean by the word "test." When most practitioners ask about testing controls, they mean do they need to test the operating effectiveness of a control. The requirement to test the operating effectiveness of a control is very rare in an audit of a LCE. However, in every audit, an auditor will need to evaluate (aka test) the design of certain controls and they will be required to determine whether certain controls have been implemented (placed in operation).

Question 3. Does the risk assessment standard specify which controls require more testing than merely an understanding?

Answer. Yes. AU-C 315.27 requires the auditor to evaluate the design and determine the implementation of certain controls within the control activities component. The Guide uses the term "identified controls" when referring to this group of controls that meet the requirements in 315.27 and, therefore, require more work than just an understanding. Certain methodologies may refer to these controls as "relevant controls" or "key controls." These controls include the following: a. Controls that address a risk that is determined to

be a significant risk b. Controls over journal entries and other adjustments as required by AU-C 240, Consideration of Fraud in a Financial Statement Audit c. Controls for which the auditor plans to test operating effectiveness in determining the nature, timing, and extent of substantive procedures, which includes controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence d. Other controls that, based on the auditor's professional judgment, the auditor con□siders appropriate to enable the auditor to assess the risks of material misstatement at the assertion level and to design further audit procedures e. The entity's general IT controls and the risks arising from the use of IT

Question 4. What is the difference between the terms "understand," "evaluate," and "determine" as those terms are used in AU-C 315?

Answer. Unfortunately, many practitioners do not understand the nuances between certain requirements as used in AU-C 315. As you read AU-C 315, it is critical that you understand the differences between (a) an understanding, (b) an evaluation, and (c) a determination. When AU-C 315 uses the term or phrase "gaining an understanding" this means performing procedures to become knowledgeably aware of your client's controls (policies and procedures) for each of the five internal control components. Gaining an understanding does not require you to make a "good or bad," "effective or not effective" evaluation or determination about the system of internal control nor about specific controls. An understanding can be gained by performing procedures such as inquiry or reading documents prepared by management or others. For example, in obtaining an understanding of the control activities around cash, you could inquire about what policies and controls the client has to capture, account for, and record cash in a manner that complies with the accounting framework. You might also inquire about what controls the client has in place, if any, to mitigate the theft of cash. At this point, the auditor is not making any type of evaluation or determination about whether those policies and procedures are good or bad, or present or absent. The auditor is merely understanding what is or is not present. On the other hand, for every control identified pursuant to AU-C 315.27, the auditor is asked to make an "evaluation" of the design of a control. This requires the auditor to make a professional judgment about how effective the control's design is. Said in plain English, evaluating the design of an identified control involves the auditor's judgment of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements, assuming the control is implemented. For example, a client might perform monthly cash reconciliations for all cash accounts. To evaluate whether those controls are effectively designed, the auditor could examine two monthly cash reconciliations prepared by the client and evaluate the controls (that is, who prepared the reconciliation, who

reviewed and approved the process, and how exceptions are followed up on) against the control objectives and then make a professional judgment about whether the controls are designed in a way that would achieve the control objective. In trying to achieve a control objective, a client designs controls to mitigate the risk of "what can go wrong" in the pursuit of reliable financial statements. Thus, there is a direct link between your client's control objectives, the risk to achieving those objectives, and the control. Your evaluation of the design is an evaluation of whether the control(s) would effectively mitigate financial reporting risks if those controls were implemented. Finally, for each of those identified controls, an auditor is required to make a determination of whether the control has been implemented. A determination means to make a definitive decision about something. As used in AU-C 315, asking the auditor to "determine," means making a "yes or no" decision about whether a control has been placed in operation. For example, in determining whether the cash reconciliation controls have been placed in operation, the auditor is not able to rely on inquiry alone. Therefore, an auditor could perform additional procedures, such as a walkthrough, in order to examine two months of reconciliations to obtain evidence that the cash reconciliation controls are being performed (they have been implemented or placed in operation).

Question 5. Can the auditor evaluate the design of a control or determine whether it's been placed in operation by inquiry?

Answer. Inquiry alone is never sufficient audit evidence to make an evaluation about design or a determination about implementation (sometimes referred to as D&I testing). Risk assessment procedures to obtain audit evidence about the design and implementation of identified controls may include: • Inquiring of entity personnel (inquiry alone is not sufficient to determine implementation) • Observing the performance of specific controls, for example, by performing what is often called a walkthrough • Inspecting documents and reports • Reperforming the specific controls

Question 6. What is the importance of performing D&I testing?

Answer. The results of D&I testing should influence what substantive tests you perform. For example, assume you've determined that your audit client has well designed and implemented controls for accounts payable cutoff at year end. The auditor may use this risk assessment information to design different substantive cutoff procedures for that audit client compared to another audit client where such controls are not well designed. While a control can't be relied upon unless the auditor tests the operating effectiveness of that control, that doesn't mean that your evaluation of the design and determination of the implementation of identified controls can't assist in the design of the nature and timing of substantive procedures that are responsive to the related risks of material misstatement.

Question 7. When does it make sense to test the operating effectiveness of a control?

Answer. When you evaluate the design of an identified control as being effective and you determine that it has been implemented, it's possible that your audit will be more effective and efficient if you plan your further audit procedures to test the operating effectiveness of the control. Areas that may benefit from this approach include revenue and expense testing, or any area with significant sample sizes. Once an engagement team has evaluated a control's design and performed audit procedures to determine that the control has been implemented, determining operating effectiveness may not involve much more work. If control risk can be reduced (even by a little) by testing the operating effectiveness of the identified control, then the nature, timing, and extent of substantive tests can be reduced, and this may lead to a more efficient and effective audit.

Question 8. Others have told me that walk-throughs are required under SAS 145? Is that correct?

Answer. No. While there is no requirement to perform a walk-through, a well-planned, rigorous, and thorough walkthrough, done with an appropriate level of professional skepticism is an excellent risk assessment procedure to evaluate the design of an identified control and determine that it has been implemented. Walk-through procedures usually include a combination of inquiry, observation, inspection of relevant documentation, and reperformance of controls. To perform a thorough walk-through, you want to make inquiries of people who actually perform the procedure, not just someone at a supervisory level. Then, corroborate the responses to your inquiries by performing additional procedures such as the inspection of relevant documents or accounting records, or corroborating inquiries made of others. A properly performed walk-through allows you to confirm the design of identified controls over the processing of the information and to gain some evidence that the controls exist and that client personnel are using them (e.g. implemented). While a walk-through is often used to provide evidence regarding the design and implementation of identified controls, a walk-through also may be designed to include procedures that are tests of the operating effectiveness of relevant controls (for instance, inquiry combined with observation, inspection of documents, or reperformance of several transactions).

Question 9. I have a very small audit firm. Is it appropriate to have my senior (3 years of experience) perform the risk assessment procedures and fill out the forms?

Answer. Because of the unique demands of a LCE audit, experienced engagement team members need to be involved in the performance of risk assessment procedures. The job of making informed risk assessment decisions should not be left to less experienced

auditors. Having experienced engagement team members involved in making the risk assessment will not only make your audits more effective but also more efficient. Critical areas include decisions about: • The nature, timing, and extent of risk assessment procedures designed to gather information about the client and its environment, including its system of internal control • The identification and assessment of risks of material misstatement • The nature and extent of the auditor's documentation of assessed risks • The nature and extent of the documentation of the client's controls Regardless of the staff assigned to an audit engagement, they need to be reminded about the need for professional skepticism. Far too often, audit staff tend to think that their job is to "please their client" as compared to protecting the public's interest. Professional skepticism means maintaining "an attitude that includes a questioning mind, being alert to conditions that may indicate possible misstatement due to fraud or error, and a critical assessment of audit evidence."

Question 10. Is it appropriate to use Audit Data Analytics (ADAs) in lieu of Analytical Procedures?

Answer. Analytical procedures are defined in generally accepted auditing standards (GAAS) as the "evaluation of financial information through analysis of plausible relations among both financial and nonfinancial data." Analytical procedures can be performed using a number of tools or techniques, most of which will be automated. Applying automated analytical procedures to the data is sometimes referred to as audit data analytics or ADAs. In short, ADAs are techniques that can be used to perform various audit procedures, including risk assessment procedures. ADAs and analytical procedures are interrelated, but not all ADAs are analytical procedures. What's important is to use your understanding of the client's business and industry to determine plausible relationships (commonly referred to as setting expectations) before performing any analytical techniques.

Question 11. Is it appropriate to just compare current balances to the prior year for my risk assessment analytic procedures?

Answer. Understanding your client's business and environment and determining reasonable or plausible relationships go hand in hand. A common problem identified in peer review is when staff perform an analytical procedure as part of risk assessment and the expectation is that nothing will change materially from the prior year. For example, a data analytic tool is programed to "kick out" exceptions that exceed 5% from the prior year. What happens if staff are not aware that, due to changes in the business model, such as a business combination, some current year balances should exceed the prior year by 25% or more? Setting assumptions that the current year balance should be approximately the same as the prior year, staff undoubtedly will see "exceptions" that really aren't exceptions.

Or worse, they may find a balance that is approximately the same as last year, and think that's fine, when, in fact, the change should have exceeded 25%. In this example, the expectation or assumption of the relationship was inappropriate and, therefore, the analytical procedure was not effective and its performance was inefficient. This issue has been seen in audits by peer reviewers during the Covid pandemic when auditors did not take into effect how the pandemic impacted various aspects of their clients' business.

Question 12. We perform monthly bookkeeping services for several audit clients. Does the performance of these nonattest services create any unique risk assessment issues that we need to be aware of?

Answer. Because of the unique features of smaller entities, it is very common for an audit firm to be involved in performing nonattest services for an audit client. Typical nonattest services include financial statement preparation, cash-to-accrual conversions, performing or preparing reconciliations, and tax return preparation and representation. All nonattest services are subject to the interpretations under the "Nonattest Services" subtopic ("Scope and Applicability of Nonattest Services" interpretation (AICPA, Professional Standards, ET sec. 1.295.010) (formerly Interpretation No. 101-3, "Nonattest Services"). The performance of nonattest services create independence risks and also may affect professional judgments and skepticism of the audit team. Besides the obvious independence risks and the need to mitigate those risks, there also may be a higher risk that audit team members may not apply the same professional judgments and professional skepticism to accounting data if other members of the firm were involved in preparing such data. When the firm is involved in the performance of accounting and bookkeeping services for an audit client, the engagement team should be careful not to prematurely dismiss something that doesn't appear to be correct by assuming that it is correct because the firm was involved with its preparation. The bottom line in performing effective risk assessment procedures is to remember that the objective is not to just look for evidence that corroborates or supports management's amounts and disclosures. Instead, auditors need to be alert and on the lookout for risk assessment evidence that may contradict management's amounts and disclosures.