Q and A on Risk Assessment Part 1

Question 1. It seems a waste of time filling out all those risk assessment forms since I use standardized audit programs. Is it really important?

Answer. Many auditors of LCEs use standardized audit programs that result in an auditor performing the same substantive tests of balances audit after audit, year after year. While there is nothing wrong with using standardized audit programs as a starting point, those programs cannot be 100% responsive to all risks of material misstatements. Think about risk assessment procedures as a process to ferret out the higher risks that need to be addressed in a particular audit engagement. If risk assessment is viewed as a process intended to identify risks of material misstatement (RMMs) that might exist in a particular audit, the process may make more sense to those involved in performing the audit engagement. Once RMMs have been identified for a particular audit engagement, then your standardized audit programs can be tailored and designed to address those potential misstatements, while at the same time eliminating or reducing procedures in low-risk areas.

Question 2. Aren't all material accounts considered RMMs?

Answer. No. A risk of material misstatement (RMM) exists when: a) There is a reasonable possibility of a misstatement occurring (that is, its likelihood), and b) If it were to occur, there is a reasonable possibility of the misstatement being material (that is, its magnitude) To illustrate, assume that your audit client's fixed assets are very material to the entity's financial statements. But, because of their nature and that there were no additions or deletions in the current year, you believe the risk of fixed assets being materially misstated is low. Because it is your professional view that there is not a reasonable possibility of a misstatement occurring, this is not considered a RMM. Assume that another account has a very high risk of being misstated, but even if a misstatement occurs, the misstatement would not be material. By definition, this is not a RMM.

Question 3. As long as I perform all the procedures in my standardized audit program won't I detect any material misstatement?

Answer. Not necessarily. Consider a portfolio of 20 audits for small housing authorities. Typically, these audits are not overly complex, inflows are predictable rents based on signed rental agreements, and outlays consist of debt service, capital reserves, and maintenance. Transactions are minimal and predictable. However, in some of those 20 audits you could see unique financial reporting considerations such as: • Impairment of buildings and other long-lived assets due to vacancies • Going concern due to cash flow deficiencies • Asset retirement obligations from contracts • Environmental remediation

liabilities • Debt classification due to covenant violations • Risks and uncertainties disclosures, and some that might qualify as a single audit. If all 20 audits are considered the same and the auditor uses the same “cookbook” (primarily substantive approach), the likelihood exists that the unique considerations noted above will be missed. Risk assessment requirements are not designed to make the audit process more onerous; in fact, if followed and scaled appropriately, the risk assessment requirements allow auditors to be more efficient, and effective in their audits because a thorough risk assessment will allow an auditor to appropriately tailor the auditor’s procedures to support whether they have reduced audit risk to an acceptable level; while at the same time, reducing or eliminating their time and hours in areas where the risks of misstatement are low. Far too often, auditors, especially younger inexperienced staff, get tangled up in the weeds of their own checklists to the point where they lose sight of the risk assessment objective.

Question 4. Why is it important to distinguish RMMs at the financial statement level as compared to RMMs at the assertion level?

Answer. Because an auditor will assess and respond to RMMs at the financial statement level differently from RMMs at the assertion level, it’s important that your audit methodology distinguish between the two. RMMs at the financial statement level refer to risks that relate pervasively to the financial statements as a whole and potentially affect many different assertions. For example, a weakness of controls because there is a lack of qualified personnel in financial reporting roles will affect many different accounts and assertions. RMMs that do not relate pervasively to the financial statements are RMMs at the assertion level. Assertion level risks are addressed by the nature, timing, and extent of further audit procedures, which may include substantive procedures or a combination of tests of controls and substantive procedures. For example, if your risk assessment leads you to assess that there is a high inherent risk that inventory quantities are overstated, you would design further audit procedures to specifically respond to that risk. Remember, your design and performance of further audit procedures should be directly linked to your identification and assessment of the risks of material misstatement (at both the financial statement and the assertion level).

Question 5. Do I need to assess inherent risk and control risk for each account and each assertion?

Answer. No, but the auditor does need to assess inherent risk and control risk for each identified RMM at the assertion level. Remember, just because an account is material, doesn’t automatically make it a RMM. Once you have identified a RMM at the assertion level, you should assess the inherent risk by assessing the likelihood and magnitude of misstatement and, in doing so, take into account how, and the degree to which: a) Inherent

risk factors affect the susceptibility of relevant assertions to misstatement, and b) The RMMs at the financial statement level affect the assessment of inherent risk for RMMs at the assertion level Additionally, the auditor should determine whether any of the high inherent risks are significant risks. The control risk assessment, which now needs to be a separate assessment, is based on the auditor's understanding of controls and the auditor's plan to test the operating effectiveness of controls. If the auditor does not plan to test the operating effectiveness of controls, the auditor should assess control risk at the maximum level such that the assessment of the RMM is the same as the assessment of inherent risk. For example, if control risk is set at the maximum level of 100% and inherent risk is set at 70%, the RMM would be 70% (RMM=IR X CR). You would never have a RMM assessed as moderate or low when you have assessed inherent risk as high and control risk as high. Additionally, in our view, you would not assess RMM as high if you assess inherent risk as moderate or low and control risk as high. Remember, it is important that your risk assessments are supported by audit evidence. It is not appropriate to simply designate a risk (inherent or control) to be at a given level without any support for that assessment.

Question 6. I understand that the concept of a “significant risk” changed with the issuance of SAS 145, is that correct?

Answer. Yes. AU-C 315 now defines a significant risk as: An identified risk of material misstatement: • For which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur, or • That is to be treated as a significant risk in accordance with the requirements of other AU-C sections As this new definition implies, not all “high” inherent risks are the same and not all high inherent risks are significant risks. While auditors have traditionally ranked inherent risk on a spectrum (such as high, moderate, low), there wasn’t explicit recognition of an inherent risk spectrum in the standards prior to SAS 145. The revised definition of significant risks should further assist auditors in identifying which inherent risks also are significant risks.

Question 7. How do I decide whether a high inherent risk is or is not a significant risk?

Answer. Auditors will use the combination of the likelihood and magnitude of a possible misstatement in making a professional judgment as to where on the spectrum of inherent risk a specific inherent risk falls. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean that both the magnitude and likelihood need to be assessed as high. Rather, it is the intersection of the magnitude and likelihood

of the material misstatement on the spectrum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the spectrum of inherent risk. A higher inherent risk assessment (i.e., a significant risk) also may arise from different combinations of likelihood and magnitude, for example, a higher inherent risk assessment could result from a lower likelihood but a very high magnitude.

Question 8. What are inherent risk factors? Is this a new term in SAS 145?

Answer. Yes. SAS 145 introduces a new concept of inherent risk factors. While auditors have always been aware of factors that increase inherent risk, those factors now have a name. Think about inherent risk factors as the factors that subject an assertion about a class of transactions, account balance, or disclosure to the susceptibility to misstatement, before considering controls. As inherent risk factors, such as complexity and subjectivity, are more present or are higher among different assertions, so too will inherent risk increase or be higher (see chapter 5 of the Guide for further discussion about inherent risk factors). Inherent risk factors are intended to assist the auditor in focusing on those aspects of events or conditions that affect an assertion's susceptibility to misstatement, which, in turn, facilitates a more focused identification of risks of material misstatement at the assertion level. Understanding the degree to which inherent risk factors affect susceptibility of assertions to misstatement will assist the auditor in assessing inherent risk, which also informs the auditor's design of further audit procedures in accordance with AU-C section 330, Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.

Question 9. Our audit methodology classifies inherent and control risks along a spectrum of low, medium, or high. Do we need to change our audit methodology to distinguish and document which high inherent risks are significant risks?

Answer. Nothing in SAS 145 requires a firm to change its existing audit methodology. It is up to each auditor, using their professional judgment, to decide which high inherent risks are at the higher end of the inherent risk spectrum and thereby deemed to be significant risks. To make this process easier and documentation clearer, some firms are adding a new level such as “higher” or “elevated” to their methodology. This new level is used to distinguish which high inherent risks are considered significant risks. Regardless of the methodology used, it is important that the auditor document which high inherent risks are also significant risks and why.

Question 10. My audit practice consists of auditing small entities that are very simple businesses. Is it possible not to have any significant risks?

Answer. The concept of significant risk is unrelated to the size of an entity. Rather, your inherent risk assessment is based on the likelihood and magnitude of a misstatement without taking into account any controls that the entity might have. We expect that almost every audit will have several significant risks, including at least one significant risk due to fraud for revenue recognition. This view is consistent with the AICPA's Special Peer Reviewer April 2022 Alert, which indicates that "virtually every audit, including audits of small- and medium-sized entities, has at least one significant risk." As a reminder, AU-C 240, Consideration of Fraud in a Financial Statement Audit, specifically AU-C 240.27 still indicates, in part, that the "auditor should treat those assessed risks of material misstatement due to fraud as significant risks ...."

Question 11. Because most smaller entities have an unsophisticated and undocumented system of internal control, it is difficult to obtain an understanding of the system of internal control. Does the Guide explain why this understanding is important and what information we need to be looking for?

Answer. The reason an auditor is asked to gain an understanding of the system of internal control is so that they understand what controls are present as well as what controls are not present (areas where there is an absence of controls). The knowledge of your client, including your understanding of the system of internal control, will help you to identity and assess the risks of material misstatement in the financial statements that you are auditing. These risks are often expressed in simple terms of "what can go wrong" in specific classes of transactions, account balances, and assertions and disclosures. For example, if your understanding of controls leads you to believe that your client has no effective controls over the cut-off of year-end accounts payables, your audit procedures will be more encompassing compared to those audit procedures performed for a client that does have well designed and implemented controls over year-end payable cutoffs. This example is an illustration of the importance of understanding controls to design effective audit procedures even in cases where control risk will be assessed at maximum.

Question 12. Is my client required to use the COSO internal control framework?

Answer. No. There are no requirements in U.S. generally accepted accounting principles (U.S. GAAP) nor generally accepted auditing standards (GAAS) that require management to use any specific internal control framework. However, GAAS is consistent with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in its use of the five components and their definitions. Therefore, it is recommended that every auditor be familiar with the COSO framework and its principles. AU-C 315 requires the auditor to gain an understanding of the entity's system of internal control. So, for purposes of GAAS, the system of internal control consists of five interrelated components, which are the same

as in COSO framework. They are: i. Control environment ii. The entity's risk assessment process iii. The entity's process to monitor the system of internal control iv. The information system and communication v. Control activities While not required, the COSO principles provide a very good framework to use in helping an auditor gain an understanding of what policies and procedures should exist in each of the five components.

Question 13. If my small business clients have policies and procedures that address the recording and reporting of financial information, are these policies and procedures considered controls?

Answer. Auditors, especially those less experienced, have often failed to understand that controls are nothing more than policies and procedures. One important change in SAS 145 was to define "controls" and to also define the "system of internal control." Controls are defined as policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context: • Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. • Procedures are actions to implement policies. Said in plain English, controls, relating to financial reporting, are policies or procedures that an entity establishes to either prevent (commonly known as preventive controls) or detect and correct in a timely manner (commonly known as detective controls) a material misstatement of its financial statements, regardless of the basis of accounting used by the entity. A system of internal control is defined as the system designed, implemented, and maintained by those charged with governance, management, and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.