Center for Plain English Accounting: Risk Assessment FAQs

The Center for Plain English Accounting (CPEA) is the AICPA's national A&A resource center. The CPEA's team of experts assists member firms in understanding and implementing accounting, auditing, review, compilation and quality control standards by sharing technical advice and guidance in a straightforward manner.

Through CPEA's extensive work with member firms, they have compiled the following list of frequently asked questions (FAQs) to aid practitioners in complying with AU-C Section 315.

Why put the time and effort into risk assessment? What's the point?

The auditing risk assessment requirements were not designed to make the audit process more onerous; in fact, if followed appropriately, those requirements should allow auditors to appropriately tailor their procedures to ensure they have reduced audit risk to an acceptable level. When auditors perform the same substantive tests of balances year after year, there could be significant risks that are not properly addressed by the audit process.

What are the objectives of risk assessment?

The risk assessment process is important for every audit, regardless of the size or industry in which the reporting entity having financial statements audited operates. Two key objectives of the risk assessment process are:

- Obtaining an understanding of the client and its environment, including an understanding of internal control relevant to the audit; for those controls that are relevant, auditors are required to evaluate the design of those controls, including relevant control activities, and determine whether the controls have been implemented
- Designing further audit procedures that are clearly linked and responsive to the risks identified

What is the "top-down" approach and why should auditors follow it?

Auditors should approach the risk assessment process from the "top down" as follows:

- Obtain an understanding of the client and its environment
- Obtain an understanding of internal control relevant to the audit

- Brainstorm with the engagement team about the risks of material misstatement due to fraud or error
- Document specific risk assessments and planned responses, including whether additional procedures will be necessary

This “top-down” approach is more effective and efficient when compared to using a methodology where auditors approach balances and transactions from the “bottom up.” Essentially, a top-down approach allows auditors to better focus and identify significant risk areas and plan more effective and efficient audits.

What questions should auditors ask themselves about their current audit methodology?

A couple of key questions that auditors should ask are:

- Does the audit methodology used require completion of a series of checklists that do not seem to add any value to the audit?
- Do engagement team members have a lack of understanding as to why checklists that are utilized need to be completed?

If the answer to either of the above-noted questions is yes, auditors should take a critical look at the purpose of utilizing the checklists and whether the checklists really are helpful in the risk assessment process. In audits of many smaller, nonpublic entities, it is likely that drafting relatively simple memos would be sufficient such that there is no need to use the checklists.

Use of checklists is not required by the auditing standards, but they simply are tools many auditors use to ensure they have followed all the steps that need to be completed in an audit. In some cases, these checklists appear to overcomplicate the process and result in many “no” or “not applicable” responses. They also are not typically tailored to a specific client or industry and may not address all significant risks and issues that need to be addressed in a particular audit.

What are the key steps to perform when assessing and responding to risks of material misstatement?

Auditors should:

- Assess the risks of material misstatements at both the financial-statement and relevant assertion levels.

- Determine which risks are significant and the assertions affected.
- Determine what controls, either individually or in the aggregate, are designed and implemented to mitigate significant risks.
- Design specific procedures that are responsive to significant risks; where client controls likely would mitigate significant risks, consider whether those controls should be tested as part of further audit procedures.
- For non-significant risks, design further audit procedures where the nature, timing and extent of those procedures are responsive to the assessed risks of material misstatement; these risks often are addressed through standard audit work program procedures.
- Provide a clear linkage between the risk assessments and the nature, timing and extent of the further audit procedures.

What are significant risks and why should auditors focus on them?

Significant risks are defined as those risks of material misstatement that require special audit consideration. Significant risks often relate to significant nonroutine transactions and matters that require significant judgment; routine noncomplex transactions that are subject to systematic processing are less likely to give rise to significant risks.

In exercising professional judgment to determine whether a risk is significant, auditors need to consider:

- The nature of the risk
- The likely magnitude of potential misstatement, including the possibility that the risk may give rise to multiple misstatements
- The likelihood of the misstatement occurring

At times, it appears that audits are performed in a manner such that there is a lack of focus on significant risks when compared to other risks of material misstatement in the financial statements. While there is nothing wrong with using standard audit work programs, those programs cannot be 100 percent responsive to significant risks, as they require additional audit consideration above and beyond the standard audit approach. Once significant risks have been identified for a particular audit engagement, then audit work programs can be better designed and tailored to address and mitigate significant risks.

Auditors might utilize about 90 percent of their time on risks that are not deemed significant, and 10 percent of their time on the significant risks, whereas the reverse should be true. If auditors performed appropriate risk assessments and responded accordingly to those risks, significantly more time would be utilized in addressing significant risks with less time devoted to the remaining risks that have not been deemed significant.

Is it OK to default to maximum control risk without obtaining an understanding of internal control?

One of the most common misconceptions when it comes to audits of smaller, nonpublic, less complex entities is that it is appropriate to default to control risk assessments at the maximum level. With the risk assessment requirements, defaulting to control risk assessments at the maximum level is no longer permitted.

Auditors are required to obtain an understanding that is sufficient to enable evaluation of the design of controls that are relevant to the audit. Auditors must also determine whether the controls, either individually or in combination, are capable of effectively preventing, or detecting and correcting, material misstatements in the financial statements. Additionally, they should determine that the controls have been implemented, that is, that the controls exist and that the entity having financial statements audited is using those controls.

What if the client has no controls?

On occasion, auditors follow an approach where they do not obtain the required understanding on the basis that there is the belief that the reporting entity has no controls. Even the smallest of reporting entities has some controls, although they may be just high-level controls that allow, as an example, the bookkeeper to properly code and classify cash transactions. Additionally, business owners almost always monitor business results. Then, business owners, as part of the control environment, often communicate to employees the importance of doing things right. While high-level, these are controls.

Given that a control is any policy or procedure used by a reporting entity to prevent, or detect and correct, a misstatement, auditors who claim that reporting entities have no controls are effectively saying that the reporting entities have no ability to prevent, or detect and correct, any type of misstatement that could appear in the financial statements. Focusing on that assertion, the question then exists as to how auditors ever could perform enough audit procedures and do enough testing if the reporting entity is not able to prevent, or detect and correct, any misstatement.

What if controls are not documented?

At smaller nonpublic entities, there may be certain controls that have been put in place, but those controls have not been properly documented. For example, perhaps checks are initiated and mailed by the secretary and then signed by the controller, and then the general accountant performs the monthly bank reconciliations. In these types of situations, reporting entities have established some controls regarding who has access to the checks and who has the authority to sign the checks. They have even set up a monitoring control by having the general accountant perform the monthly reconciliations. However, they have not formally documented this control.

This lack of client documentation does not necessarily mean that the control should not be tested. In some cases, it may be up to auditors to identify any controls that have been established by the reporting entity and document those controls accordingly.

Where the reporting entity lacks documentation of controls, auditors might want to issue a management recommendation that they have a formal documentation process for any controls they have established and placed in operation. It is just as important for management to understand controls and risk just as much as it is for the auditor to understand these concepts.

Do auditors need to test the operating effectiveness of controls if they don’t plan to rely on them to reduce substantive testing?

For controls that are relevant to the audit engagement, auditors need to ensure that the controls are evaluated from a design and implementation perspective. While auditors do not need to test the operating effectiveness of controls where no reliance is planned to be placed on those controls, care needs to be exercised not to inadvertently rely on high-level or other controls without testing their operating effectiveness. For example, auditors might inadvertently rely on reporting entity controls to code and classify transactions without any type of control testing.

What risk assessment documentation is required?

It is important for auditors to document their understanding of the entity and its environment, including its internal control, their assessment of the entity’s risks and how they plan to mitigate those risks. For each audit area (e.g., cash, accounts receivable, etc.), auditors should document:

- Any identified significant risks
- The assertions affected

- Assessments of inherent risk and control risk and the risk of material misstatement for relevant assertions
- Audit procedures beyond the standard work program procedures needed to mitigate the risks identified
- Linkage of the audit procedures in the work program to these risks (cross-referencing)

Audit documentation should be developed in a manner such that a professional not involved in the audit engagement, or a peer reviewer, could properly identify significant risks and other risks as well as how those risks were reduced through audit testing. To that end, documentation needs to reflect the fact that the risk assessments were performed, the results of those risk assessments and the procedures that will be performed as a result of those risk assessments.