Audit advisory

Performing risk assessments in employee benefit plan audits

This advisory is intended to inform members of recent AICPA Peer Review Board (PRB) findings and guidance related to risk assessment and what members can expect to hear from their peer reviewer about risk assessment, and to assist members in properly applying the risk assessment standards in employee benefit plan (EBP) audits.

More than a decade after the standards were issued, many auditors continue to struggle with properly implementing risk assessment procedures. The risk assessment standards establish requirements and provide guidance concerning, among other things, the auditor's assessment of the risks of material misstatement (RMMs) in a financial statement audit and the design and performance of audit procedures whose nature, timing, and extent are responsive to the assessed risks.

The PRB has found that auditors of all types of entities, including EBPs, have misconceptions about applying the risk assessment standards resulting in non-compliance. Accordingly, audit firms can expect increased scrutiny by peer reviewers of their approach to performing and documenting compliance with the risk assessment standards (in particular AU-C sections 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatemen*t, and 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*).

This advisory:

- Identifies the key steps to perform when assessing and responding to RMMs
- Highlights common areas of nonconformity in performing risk assessments
- Describes misconceptions in performing risk assessments in EBP audits
- Provides questions to consider in evaluating whether an auditor has complied with the risk assessment standards
- Discusses guidance for peer reviewers to evaluate auditor non-compliance with the risk assessment standards
- Outlines steps to help your firm evaluate whether the risk assessment standards are met
- References resources and tools to help auditors apply the risk assessment standards in EBP audits

Key steps to perform when assessing and responding to RMMs

The key steps to assessing and responding to RMMs include the following:

- Assess RMMs at *both* the financial-statement and relevant assertion levels.
- Determine which risks are significant and the assertions affected.

- For significant risks, determine what controls, either individually or in the aggregate, are designed and implemented to mitigate such 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 RMMs not assessed as significant risks, design audit procedures where the nature, timing and extent of those procedures are specifically responsive to the assessed RMMs.
- Provide a clear linkage between the risk assessments and the nature, timing and extent of the further audit procedures.

Common areas of nonconformity in performing risk assessments

The most common instances of noncompliance with risk assessment requirements found in peer reviews relate to the following areas:

Failure to gain an understanding of internal control when identifying client's risks

- Auditors are expected to perform the following steps when gaining an understanding of internal control; an audit omitting one or more of these steps results in non-compliance with AU-C 315:
    - Consider what could go wrong as the client prepares its financial statements
    - Identify the controls intended to mitigate those financial reporting risks
    - Evaluate the likelihood that the controls are capable of effectively preventing or detecting and correcting material misstatements.
- Some auditors may inappropriately indicate that the requirements of AU-C 315.14 do not apply to their client because their client has no controls.
- Auditors may erroneously default to control risk at the maximum level without gaining an understanding of the client's internal control. This is not permitted under the current Risk Assessment Standards, even when not intending to rely on tests of controls.
- Auditors may inappropriately reduce control risk to less than high without appropriately testing relevant controls.

Insufficient risk assessment

- Regardless of the nature and extent of substantive procedures, performing the audit in accordance with GAAS includes the following requirements for each engagement; omitting one or more of these requirements results in non-compliance
    - Identify the client's risks of material misstatement (RMM) by gaining an understanding of the client and its internal control (Identify RMM)
    - Assess the risks (Assess RMM) and
    - Design or select procedures that respond to those risks (Respond to RMM).
- Regardless of the size of the entity, failure to identify at least one significant risk almost always represents a failure to comply with AU-C 315.28. AU-C 240.26 states there is a presumption that risks of fraud exist in revenue recognition, and under AU-C 240.27 states risks of material misstatement due to fraud should be treated as significant risks.
- Failure to assess risk of material misstatement at *both* the financial statement level (meaning to assess risks which are pervasive to the financial statements, like a lack of expertise in the accounting department) *and* relevant assertion-level for significant classes of transactions, account balances or disclosures (meaning to assess risk for assertions that have a reasonable possibility of material misstatement, not every assertion for every account) represents non-compliance with AU-C 315.26.

- Some auditors are documenting RMM at the audit area level for every audit area, citing the risk assessment is the same for all assertions, when risks vary by assertion or not all assertions are relevant.

Failure to link procedures performed to the risk assessment

- Audit procedures should be responsive to the client's financial statement- and relevant assertion-level risks for significant classes of transactions, account balances or disclosures. The linkage is at the assertion (not account) level.
- Some auditors are performing the risk assessment in accordance with AU-C 315 but designing the audit procedures with little regard for the results of that assessment. If the risks are not properly reduced to an acceptably low level, the auditor hasn't complied with the standards.

Misconceptions in performing risk assessments in EBP audits

The following are common misconceptions in applying the risk assessment standards in EBP audits:

- Auditor can "place reliance on the SOC report" without evaluating the design and implementation of the plan's controls including management SOC user controls.
- Auditor can forego obtaining an understanding of controls at a service organization and plan sponsor and instead take a "full substantive" approach.
- Risk is assessed at the audit area, not the financial statement and assertion level.
- Because the plan's investment custodian "certified the information in the financial statements," overall audit risk was "very low" and no formal risk assessment was required.
- The overall audit risk should be assessed at low for all limited scope audits as long as the auditor obtained the custodian's certification and SOC report (e.g. valuation assertion for hard to value assets)

Questions to consider in evaluating whether an auditor has complied with the risk assessment standards

The following questions and considerations will help auditors evaluate compliance with AU-C sections 315 and 330:

1. *Did the auditor evaluate the design and implementation of controls relevant to the audit?*

   AU-C section 315.14 states when obtaining an understanding of controls that are relevant to the audit, the auditor should evaluate the design of those controls and determine whether they have been implemented by performing procedures in addition to inquiry of the entity's personnel.

2. *Did the auditor identify one or more significant risks?*

   Significant risks are RMMs that require special audit consideration. These are typically non-routine transactions that require significant judgment, such as the application of new accounting principles or valuations of hard-to-value assets. Every audit, including audits of small- and medium-sized entities, almost always has at least one significant risk. This is because, in accordance with AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*, the risk of management override of controls is present in all entities. Due to the unpredictable way in which such override could occur, it is a RMM due to fraud and, thus, a significant risk.

3. *Was risk assessed at both the financial-statement and relevant assertion levels?*

   The assessment of the RMMs is not performed solely at the account level. This is because audit responses are tied to assertion level risks, and each account may have multiple assertions which may have different levels of risk and require different audit responses. Some auditors confuse account-level risk with financial statement-level risk. Financial statement-level risks are not risks limited to one account balance, but rather, risks that are pervasive to the financials. For example, one financial statement-level risk would be a lack of expertise in the client's accounting department, which would affect numerous accounts and assertions. Financial statement-level risks require an overall response, such as assigning more experienced audit staff or incorporating additional elements of unpredictability.

4. *Are the assessed levels of the RMM and the designed response appropriate in the auditor's professional judgment?*

   The objective of risk assessment is to allow the auditor to design responses specific to the risk identified. Generally accepted auditing standards do not ordinarily refer to inherent risk and control risk separately, but rather to a combined assessment of the RMM. However, the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations. The assessment of the RMM may be expressed in quantitative terms, such as in percentages, or in nonquantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made. Designing the right response to RMM is more important than whether the risk was high, low, moderate or any other ranking of risk.

5. *Is there a clear linkage between risk assessment and response?*

   Many auditors of smaller clients appear to be documenting their risk assessment in accordance with AU-C section 315, but performing procedures with little regard to the results of that assessment. This is often due to overreliance on standardized, third-party practice aids. While standardized practice aids can be valuable tools, to be effective they must be used as intended. Even if an auditor uses standardized aids, they are still required to link the procedures they perform back to their risk assessment. Auditors should consider the linkage between the risk assessment and the auditor's procedures, and they should determine whether the procedures are responsive to the client's financial statement- and assertion-level risks.

6. *Were special audit considerations performed for significant risks?*

   AU-C section 315.04 defines "significant risk" as an identified and assessed RMM that, in the auditor's professional judgment, requires special audit consideration. AU-C section 330.22 states the auditor should perform substantive procedures that are specifically responsive to significant risks, and that when the approach to a significant risk consists only of substantive procedures, those procedures should include tests of details. In addressing significant risks, if an auditor has not performed audit procedures that are not part of the auditor's standard approach, the audit could fail to comply with AU-C section 330.22. AU-C section 315.29 states in exercising professional judgment about which risks are significant risks, the auditor should consider at least risks relating to fraud, recent economic accounting or other developments, complex or related party transactions, measurement uncertainty, and significant and unusual transactions.

Peer Review guidance for peer reviewers to evaluate auditor non-compliance

In September 2018 (and revised in October 2018), the Peer Review Board approved a new section to PRPM Section 3100, *Supplemental Guidance*, entitled, "*Evaluation of Non-compliance with the Risk Assessment Standards*." The Peer Review guidance provides considerations for the reviewer to use

when evaluating the auditor's compliance with the AU-C sections 315 and 330, defines the peer review impact when non-compliance is identified with those standards, and instructs peer review Report Acceptance Bodies (RABs) to require certain implementation plans or corrective actions when Findings for Further Consideration forms or deficiencies in the peer review report are issued. Members should be aware that the guidance indicates that if a peer reviewer finds non-compliance with the Risk Assessment Standards, that engagement should be deemed "non-conforming". The guidance is effective for peer reviews commencing on or after October 1, 2018 through reviews commencing on or before September 30, 2021.

The peer reviewer guidance is available on the AICPA Peer Review website at https://www.aicpa.org/content/dam/aicpa/interestareas/peerreview/newsandpublications/downloadabledocuments/reviewer-alert-201810.pdf

Steps to help your firm evaluate whether the risk assessment standards have been met

The following are suggested steps that your firm can take to evaluate whether the risk assessment standards have been met:

1. Review the requirements of AU-C sections 315 and 330 to gain a full understanding of the requirements in the standards.
    - AU-C section 315 addresses the auditor's responsibility to identify and assess the RMMs in the financial statements through understanding the entity and its environment, including the entity's internal control.
    - AU-C section 330 addresses the auditor's responsibility to design and implement responses to the RMMs identified and assessed by the auditor in accordance with AU-C section 315.

2. Use the AICPA Audit Guide, *Assessing and Responding to Audit Risks in a Financial Statement Audit*, which is a source for guidance on applying the core principles of the risk-based audit methodology required for all financial statement audits.

3. Review the guidance on audit risk assessment and internal control in Chapters 3 and 4, respectively, in the AICPA Audit and Accounting Guide, *Employee Benefit Plans* (EBP Guide). The EBP Guide includes examples of the more common identified risks of what can go wrong at the relevant assertion level and example audit procedures to address those risks. Chapter 3 addresses the auditor's risk assessment in an audit of an EBP, including understanding the entity and its environment, including its internal control; risk assessment procedures and risk assessment; audit procedures responsive to the assessed RMMs; and an overall response. Chapter 3 also identifies potential pervasive risks for EBP audits at the financial statement level, and areas that may present particular RMMs at the assertion level for classes of transaction, account balances, and disclosures, when auditing EBPs. Chapter 4 discusses the understanding of the plan's internal control as part of the risk assessment and provides examples of activities related to EBPs that may include controls (both manual and automated IT) relevant to the audit.

4. Perform a self-inspection of your firm's risk assessment approach using the free AICPA Internal Inspection Practice Aid, *Addressing Non-Compliance with AU-C 315 and 330,* to evaluate whether the requirements of AU-C sections 315 and 330 are met.

5. Use the free AICPA Audit Risk Assessment Tool as a supplement to the auditor's existing planning module, whether in an auditor-based or commercially provided methodology. The Audit Risk Assessment Tool is recommended for use on audit engagements that are generally smaller in size and have less complex auditing and accounting issues. It is designed to help identify risks,

including significant risks, and document the planned response to those risks. The Audit Risk Assessment Tool is not a complete planning module. *[The AICPA recommends that audit professionals with substantial accounting, auditing and specific industry experience and knowledge complete the Audit Risk Assessment Tool. For an auditor to be successful in improving audit quality and efficiencies, it is recommended that a 5+ years experienced auditor complete the Audit Risk Assessment Tool or the engagement team member with the most knowledge of the industry and client (often Partner in small/medium auditors) provide insight to whomever is completing the ARA Tool.]*

6. Provide training to your audit staff on proper risk assessment and response as well as common misconceptions to avoid. The AICPA has developed a free PowerPoint presentation with speaker notes and a case study to use for staff training: Staff Training Workshop Presentation (PPT). The AICPA also offers a self-study CPE course which walks through the most pervasive issues that peer reviews have found and how to avoid them in your practice: Risk Assessment Deep Dive: How to Avoid Common Missteps.

7. Use other risk assessment tools and resources available in the AICPA Risk Assessment Resource Center and the EBPAQC Risk Assessment Resource Center.

8. Discuss your firm's approach to performing and documenting risk assessment with your firm's peer reviewer.