

# RISK ASSESSMENT

NCACPA 2022 Symposium  
Conference

*Michael Manspeaker, CPA*  
*Coastal Peer Review, Inc.*



**Coastal Peer Review**

Administered by The North Carolina and  
Maryland Associations of CPAs

# Learning Objectives

- Overview Of Risk Assessment Process
- Introduction to SAS 145



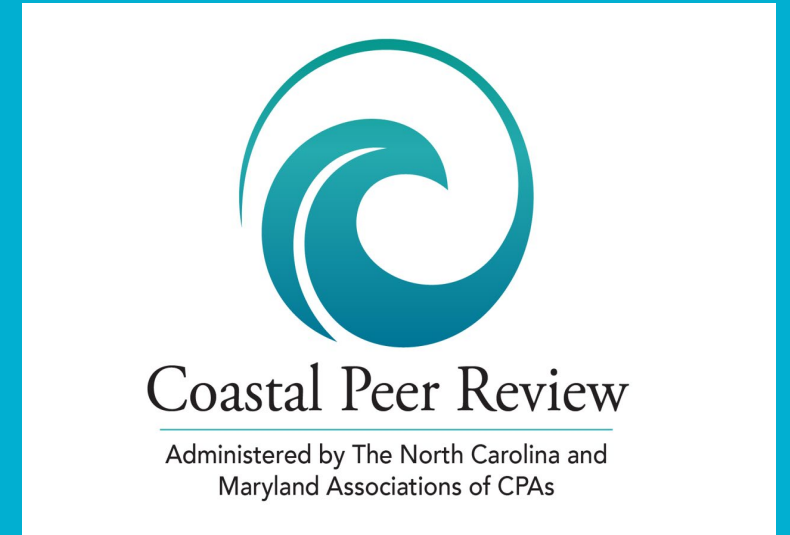
Coastal Peer Review

Administered by The North Carolina and  
Maryland Associations of CPAs

# Coastal Peer Review, Inc.

Before 2021, the NC Association of CPAs and the Maryland Association of CPAs each administered peer reviews in their respective states.

Changes to peer review administration beginning in 2017 caused most peer review administering entities to reimagine their process and organization.



# Coastal Peer Review, Inc.

In June 2020, both the North Carolina Association of CPAs Board of Directors and the Maryland Association of CPAs Board of Directors approved joint peer review administration through a newly created entity, Coastal Peer Review, Inc.

The Coastal Peer Review Committee and RABs have members from both NC and MD.



# Peer Review Issue !

- Deficiencies in the auditor's risk assessment procedures are a common issue identified by practice monitoring programs in the United States and worldwide.
  - In 2020 U.S. peer reviews, the currently effective AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, was the leading source of *matters for further consideration*

# *SAS 145, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*

## Why?

- Significant area of peer review findings
- Challenges related to the extent to which understanding of internal control is necessary
- Scalability concerns and challenges

© 2023



# SAS 145

- In October 2021, the AICPA Auditing Standards Board (ASB) issued Statement on Auditing Standards No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*

# SAS 145

- SAS No. 145 does not fundamentally change the key concepts underpinning audit risk. Rather, it clarifies and enhances certain aspects of the identification and assessment of the risks of material misstatement to drive better risk assessments and, therefore, enhance audit quality.



# Overview of SAS 145

- Enhances requirements and guidance related to obtaining an understanding of the entity's system of internal control and assessing control risk
- Includes revised requirements to evaluate the design of certain controls within the control activities component, including general information technology (IT) controls, and to determine whether such controls have been implemented.

# Overview of SAS 145

- Revises the definition of significant risk
- Spectrum of Inherent Risk
- Includes a new requirement to separately assess inherent risk and control risk
- A new requirement to assess RMM such that, if the auditor does not plan to test the operating effectiveness of controls, the assessment of the risk of material misstatement is the same as the assessment of inherent risk (Control risk is at the maximum level)
- Relevant Assertions
- Significant Class of Transactions, Account Balances or Disclosures
- A risk of material misstatement 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). There is a reasonable possibility when the likelihood of a material misstatement occurring is more than remote. If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion.

# SAS 145

## Major areas of revision (cont'd)

- 5 new inherent risk factors: subjectivity, complexity, uncertainty,, change and susceptibility to misstatement due to management bias or fraud.
- Requiring separate assessments of inherent and control risk
  - If no tests of controls are performed, RMM = IR
- Requiring for “sufficient, appropriate” evidence as basis for risk assessment
- Stand-back requirement for material COTABODs not assessed as significant

# Overview of SAS 145

- A new “stand-back” requirement intended to drive an evaluation of the completeness of the auditor’s identification of significant classes of transactions, account balances, and disclosures
- Revised requirements relating to audit documentation
- New guidance on scalability;
- New guidance on maintaining professional skepticism

SAS No. 145 is effective for audits of financial statements for periods ending on or after December 15, 2023. Early implementation is permitted.

# Concept of Spectrum of Inherent Risk

- Significant Risks
- Significant Class of Transactions, Account Balances, or Disclosures
- Relevant Assertions

# Relevant Assertions

- New Definition
- –An assertion about a class of transactions, account balance, or disclosure is relevant when it has an identified risk of material misstatement, taking into account the likelihood and magnitude of a misstatement
- Old Definition
- –A financial statement assertion that has a reasonable possibility of containing a misstatement or misstatements that would cause the financial statements to be materially misstated. The determination of whether an assertion is a relevant assertion is made without regard to the effect of internal controls.

# Relevant Assertions

- A risk of material misstatement 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). **There is a reasonable possibility when the likelihood of a material misstatement occurring is more than remote.** If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion.

# SAS 145 Risk Assessment

- •New guidance on scalability
- –Complexity of an entity’s activities and its environment, including its system of internal control, is the primary driver of scalability in the application of SAS 145
- –SAS 145 has removed the “Considerations Specific to Smaller Entities” sections previously included in the application material but has incorporated most of that content elsewhere in the standard, as appropriate, together with further revisions to promote scalability
- –The AICPA Guide, *Assessing and Responding to Audit Risk in a Financial Statement Audit*, will be revised to reflect SAS 145
- –We expect that Guide to be helpful to practitioners who must “scale” and apply the provisions of SAS 145 to audits of small businesses



# Risk assessment

## Resources

- Risk Assessment Toolkit: [aicpa.org/riskassessment](https://aicpa.org/riskassessment)
- Audit risk assessment tool (includes videos)
- Self-study CPE and staff training materials
- Internal inspection aid
- Frequently asked questions

## Peer Review Implications

- Temporary guidance related to assessing noncompliance is effective for peer reviews commencing on or before September 30, 2021
- Reviews commencing subsequent to this end date are subject to normal peer review guidance



The goals of identifying, assessing and responding to risk are at the core of every audit. Identifying and assessing a client's specific risks drives the audit procedures you should perform and helps you avoid inefficient over-auditing. Even more seriously, this process helps you avoid a failure to obtain sufficient appropriate audit evidence to support your opinion.

The Audit Risk Model: Your First Step In Risk Assessment

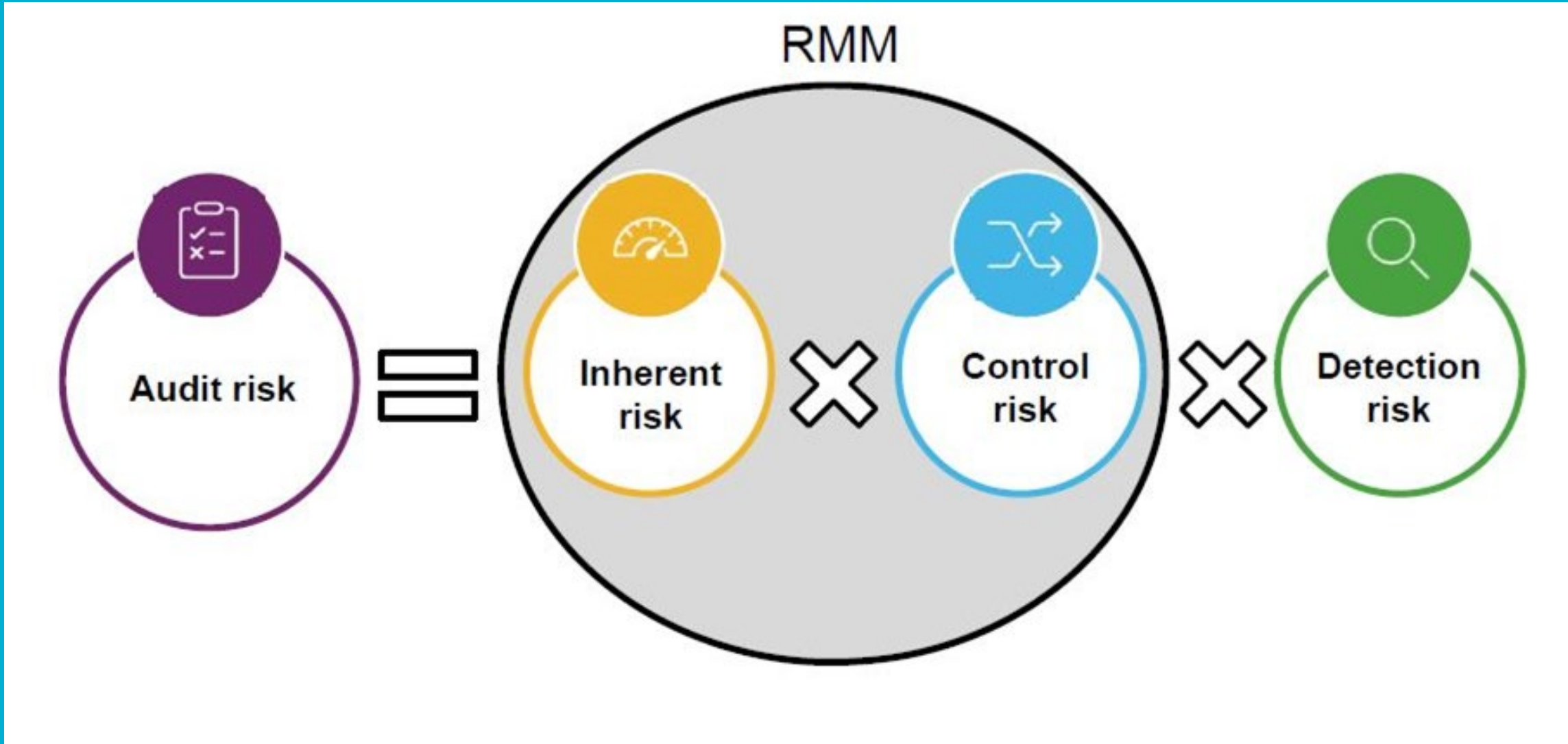
*Bob Dohrer, AICPA Chief Auditor, American Institute of Certified Public Accountants*

# ***Don't be Afraid to Ask Questions***

To plan your audit, you need to identify your client's specific risks. To identify the risks, you'll need to gain an understanding of the entity, and that means asking lots of questions. It also means keeping your eyes and ears open, observing the client and getting a good feel for their environment. The last thing you want is for a risk to go undetected. So, if you are unsure of something or need clarification, don't be shy – ask questions.

The Audit Risk Model: Your First Step In Risk Assessment

*Bob Dohrer, AICPA Chief Auditor, American Institute of Certified Public Accountants*



The Audit Risk Model: Your First Step In Risk Assessment  
*Bob Dohrer, AICPA Chief Auditor, American Institute of Certified Public Accountants*

# ***Inherent Risk***

- Inherent risk is the susceptibility of an assertion about a class of transactions, account balance, or disclosure to misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.
- Is the auditor's basis for the assessed levels of risk documented in the working papers?

## Reducing inherent risk

### **Inherent risk cannot be reduced based on competency of accounting staff**

- Inherent risk: risk of a material misstatement assuming *no related controls*
- Control risk: risk that a misstatement would not be prevented or detected and corrected by an entity's internal control
- Staff competency = part of control environment

# ***Control Risk***

- Control risk is the risk that a misstatement that could occur in an assertion about a class of transactions, account balance, or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control. An assessment of control design and implementation is required on every audit, whether or not controls are tested and relied on. Specifics regarding the account being reviewed should consider the inherent risks and whether specific controls exist to address the inherent risk by assertion.

# ***Risks of Material Misstatement***

- Risks of material misstatement exist at two levels: (1) the overall financial statement level and (2) the assertion level for classes of transactions, account balances, and disclosures. Risks of material misstatement at the assertion level consist of two components; inherent risk and control risk.



Risk assessment is fundamental.

Audit



Identifying  
risk



Assessing  
risk



Responding  
to risk



# ***Risk Assessment Procedures***

The auditor should perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement.

The risk assessment procedures should include the following:

- a. Inquiries of management and others within the entity
- b. Analytical procedures
- c. Observation and inspection

# ***Understanding the Entity and Its Environment***

The auditor should perform risk assessment procedures to obtain an understanding of

- a. The following aspects of the entity and its environment:
  - The entity's organizational structure, ownership and governance, its business model, including the extent to which the business model integrates the use of IT
  - Industry, regulatory, and other external factors
  - The measures used, internally and externally, to assess the entity's financial performance

## ***Understanding the Entity and Its Environment (continued)***

- b. The applicable financial reporting framework and the entity's accounting policies and the reasons for any changes thereto.
- c. How inherent risk factors affect the susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework, based on the understanding obtained in subparagraphs a and b.

The auditor should evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework.

# *Identifying Audit Areas to Assess Risk*

- Financial statement classes of transactions, account balances and disclosures
- Appropriate level of disaggregation
- Consideration of risk characteristics
- Other characteristics – when it is acceptable to group financial statement accounts/disclosures

# ***Identifying and Assessing the Risks of Material Misstatement***

To provide a basis for designing and performing further audit procedures, the auditor should identify and assess the risks of material misstatement at

- a. The financial statement level and
- b. The relevant assertion level for classes of transactions, account balances, and disclosures.

For this purpose, the auditor should

- a. Identify risks throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, by considering the classes of transactions, account balances, and disclosures in the financial statements

## Identifying “significant risks”

- AU-C 315.04: Risks that require special audit consideration
- AU-C 315.28: Based on inherent risk only
- AU-C 315.A139: Often nonroutine transactions that require significant professional judgment
  - Complex calculations
  - Application of new/complex accounting principles
  - Nonroutine related party transactions



# Significant Risks- SAS 145

---

- Risks that are close to the upper end of the spectrum of inherent risk.
- Based on inherent risk only



In exercising professional judgment about which risks are significant risks, the auditor should consider at least

- a. Whether the risk is a risk of fraud;
- b. Whether the risk is related to recent significant economic, accounting, or other developments and, therefore, requires specific attention;
- c. The complexity of transactions;
- d. Whether the risk involves significant transactions with related parties;
- e. The degree of subjectivity in the measurement of financial information related to the risk, especially those measurements involving a wide range of measurement uncertainty; and
- f. Whether the risk involves significant transactions that are outside the normal course of business for the entity or that otherwise appear to be unusual.

# Substantive Procedures

---

- The auditor should perform substantive procedures for each relevant assertion of each significant class of transactions, account balance, and disclosure, regardless of the assessed level of control risk. (AU-C 330.18)

## Responding to significant risks

- Special audit consideration = beyond the norm
- Often requires
  - Modifying standardized procedures or
  - Adding additional procedures
- One or more arise on most audits

### **Key point**

If auditors aren't tailoring audit programs to address significant risks, they're probably not complying with AU-C 330.

## ***Substantive Procedures- Pre SAS 145***

Irrespective of the assessed risks of material misstatement, the auditor should design and perform substantive procedures for all relevant assertions related to each material class of transactions, account balance, and disclosure.

## Documenting risk assessment

Auditor must document basis of risk assessment set at *any* level (AU-C 315.33)

RMM Assessment	Required to document basis of risk assessment?
1. High	YES
2. Medium	YES
3. Low	YES

# Internal Control Considerations

---

# ***Pre SAS 145- Evaluate the design and implementation of your client's controls***

On every audit, you are required to:

A. evaluate the design of controls relevant to the audit, and

A. determine whether these controls have been implemented.  
*This isn't the same thing as testing the operating effectiveness of controls.*

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.

**\*\*\*\*Most Common Peer Review Finding\*\*\*\***



# ***Understanding the Entity and Its Environment***

*Control activities relevant to the audit.* The auditor should obtain an understanding of control activities relevant to the audit, which are those control activities the auditor judges necessary to understand in order to assess the risks of material misstatement at the assertion level and design further audit procedures responsive to assessed risks. An audit does not require an understanding of all the control activities related to each significant class of transactions, account balance, and disclosure in the financial statements or to every assertion relevant to them. However, the auditor should obtain an understanding of the process of reconciling detailed records to the general ledger for material account balances. (Ref: par. .A99-.A105)

If the auditor has determined that a significant risk exists, the auditor should obtain an understanding of the entity's controls, including control activities, relevant to that risk

What if client has no controls?

All entities have controls

- How could audit risk be reduced to an acceptably low level?

## Common controls at small entities

- Strong “tone at the top”
- Owner communicates importance of quality
- Accounts reconciled monthly
- Owner reviews financial results
- Log-in credentials
- Limits on check signing
- Physical access to cash, limited inventory
- Invoices marked “Paid” to avoid double payment
- Payroll reviewed by owner
- AP system doesn't allow new vendor entry without authorization

## Evaluating operating effectiveness of controls

- Different from evaluating design/implementation:
  - Evaluate whether the controls were **effective** in **meeting their objective** throughout the **reporting period**
- Is this a required procedure?
  - Only required if placing reliance to reduce substantive testing
- No operating effectiveness? No reliance!

Why does COSO matter for small audit clients?

— *Considering the COSO Elements and Principles helps the auditor identify risks*

## COSO – Elements and Principles of Internal Control

Elements of internal control	Principles
Control Environment	<ol style="list-style-type: none"><li data-bbox="708 542 2165 592">1. Demonstrates commitment to integrity and ethical values</li><li data-bbox="708 614 1592 664">2. Exercises oversight responsibility</li><li data-bbox="708 685 1974 735">3. Establishes structure, authority and responsibility</li><li data-bbox="708 756 1821 806">4. Demonstrates commitment to competence</li><li data-bbox="708 828 1350 878">5. Enforces accountability</li></ol>
Risk Assessment	<ol style="list-style-type: none"><li data-bbox="708 921 1465 971">6. Specifies suitable objectives</li><li data-bbox="708 992 1439 1042">7. Identifies and analyzes risk</li><li data-bbox="708 1063 1261 1113">8. Assesses fraud risk</li><li data-bbox="708 1135 1796 1185">9. Identifies and analyzes significant change</li></ol>

## COSO – Elements and Principles of Internal Control

Elements of internal control	Principles
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies



# SAS 145- Primarily Indirect Controls

- Control Environment
- Entity's Risk Assessment Process
- Entity's Process to Monitor the System of Internal Control

# SAS 145- Primarily Indirect Controls

- SAS No. 145 includes requirements to understand, and evaluate certain aspects of, the control environment, the entity's risk assessment process, and the entity's process to monitor the system of internal control components. The auditor's required understanding includes the ongoing tasks and activities, or processes, geared to the achievement of the entity's financial reporting objectives.
- Audit evidence for the auditor's understanding and evaluation may be obtained through a combination of inquiries and other risk assessment procedures (for example, corroborating inquiries about the entity's processes through observation or inspection of documents). The auditor exercises professional judgment to determine the nature and extent of the procedures to be performed to meet the requirements of SAS No. 145.
- SAS No. 145 does not require the auditor to evaluate the design or determine the implementation of individual controls within these components. However, the auditor may, based on the auditor's professional judgment, identify controls within these components that address risks of material misstatement at the assertion level for which the auditor evaluates design and determines implementation

# SAS 145 –Primarily More Direct Controls but May Be Indirect Controls

## Information System and Communication

- SAS No. 145 includes a requirement to understand, and evaluate certain aspects of, the information system and communication component. For this component, the auditor's understanding includes, among other things, the flows of transactions and other aspects of the entity's information-processing activities for significant classes of transactions, account balances, and disclosures as well as the entity's communication of significant matters.
- SAS No. 145 does not require the auditor to evaluate the design or determine the implementation of individual controls within the information and communication component. It is important to note that the auditor's identification and evaluation of controls in the control activities component is focused on information-processing controls, also known as *transaction controls*.

# SAS 145- Primarily Direct Controls

## Control Activities

- SAS No. 145 includes specific requirements to understand certain controls within the control activities component that address risks of material misstatement at the assertion level.

# Control Activities

For the identified controls that address risks of material misstatement at the assertion level, the auditor is required to evaluate the design and determine whether the controls have been implemented. The identified controls include the following:

- Controls that address a risk that is determined to be a significant risk
- Controls over journal entries and other adjustments as required by AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*
- Controls for which the auditor plans to test operating effectiveness in determining the nature, timing, and extent of substantive procedures, which include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence
- Other controls that, based on the auditor's professional judgment, the auditor considers appropriate to enable the auditor to assess the risks of material misstatement at the assertion level and to design further audit procedures.

# Control Risk at Maximum

- When the auditor does not plan to test the operating effectiveness of identified controls, the auditor's evaluation of the design and determination of the implementation of controls may still assist in the design of substantive procedures. When identified controls are designed effectively and implemented, risk assessment procedures may influence the auditor's determination of the nature and timing of substantive procedures to be performed (for example, the auditor may determine to perform inspection, rather than external confirmation, or to perform procedures at an interim date, rather than at period end).
-

# General IT Controls

- SAS No. 145 now defines the terms *risks arising from the use of IT* and *general IT controls*. SAS No. 145 requires the auditor to identify general IT controls that address the risks arising from the use of IT and to evaluate their design and determine their implementation.
- Risks arising from the use of IT- Susceptibility of information-processing controls to ineffective design or operation, or risks to the integrity of the entity's information system, due to ineffective design or operation of controls in the entity's IT processes.
- General IT Controls- Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information-processing controls and the integrity of information in the entity's information system.

# General IT Controls

- General IT controls need not be identified for every IT process. General IT controls are identified based on the risks arising from the use of IT. To identify the risks arising from the use of IT, the auditor identifies the IT applications and other aspects of the entity's IT environment that are subject to such risks. Such IT applications and other aspects are identified based on the identified controls that address the risks of material misstatement at the assertion level, as described in the preceding table under "control activities." Appendix E, "Considerations for Understanding IT," of SAS No. 145 includes guidance that may be relevant in identifying IT applications and other aspects of the IT environment that may be subject to risks arising from the use of IT.
-



# SAS 145

- Standards vs. Methodology
  - Sequential order of procedures
  - Checklists and uniform processes, by themselves, are not agile or robust enough to address risks- Need to understand the Standards
  - Need to conduct a risk assessment that is robust and agile to identify RMM
  - Circumstances change- same as last year is dangerous!
  - Scalability relates to the level of complexity and risk. All risk assessments should be equally robust relative to the entity being audited.
-

# Questions and Discussion

# Becoming a Peer Reviewer

## Qualifications:

- Member of AICPA and Active CPA License
- Active in public practice at supervisory level in A&A with five years recent experience
- Associated with a firm that received a PASS report
- Knowledge of Professional Standards (including Peer Review and QC/QM standards)

***Benefits you, your firm and your profession!***