SAS 145: School District Edition

Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

Agenda

- Some Good News
- Overview
- Obtaining an Understanding of the Entity
- Obtaining an Understanding the Entity's System of Internal Control
- Identifying and Assessing Risks of Material Misstatement
- Applying the Standard

Maner Costerisan

Some Good News

Although SAS 145 supercedes and amends many existing sections of our standards, we don’t have to change much. The requirements are mostly clarifying in nature. Plus, we’ve been doing it for a few months by now.

Maner Costerisan

Overview

- Enables auditors to appropriately address the following:
  - Understanding the entity's system of internal control
    - Specifically relating to the auditor's work effort to obtain the necessary understanding
  - IT considerations, including assessing risks arising from entity's use of IT
  - Determining risks of material misstatement, including significant risks

Maner Costerisan

Overview

- Effective date
  - Audits of financial statements for the periods ending on or after December 15, 2023
- Common areas of deficiencies
  - U.S. peer review program
  - U.S. and global inspections results from audit regulatory bodies
- Inconsistencies in the interpretation and application of the standards
  - Understanding the components of the entity's system of internal control
  - Auditor's assessment of control risk
- Modernize the standard
  - Evolving business environment, including use of Information Technology (IT)
- Converge with the International Standards on Auditing (ISAs)
  - ISA 315, Identifying and Assessing the Risks of Material Misstatement

Maner Costerisan

Overview

SAS No. 145 enhances the following:

Requirements and guidance related to obtaining an understanding of the entity's system of internal control and assessing control risk.

Guidance that addresses the economic, technological, and regulatory aspects of the markets and environment in which entities and audit firms operate.

SAS No. 145 also includes revised and new requirements and guidance, including the following:

- A revised definition of significant risk
- 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
- A new requirement to separately assess inherent risk and control risk
- A new requirement to assess control risk at the maximum level 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
- 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

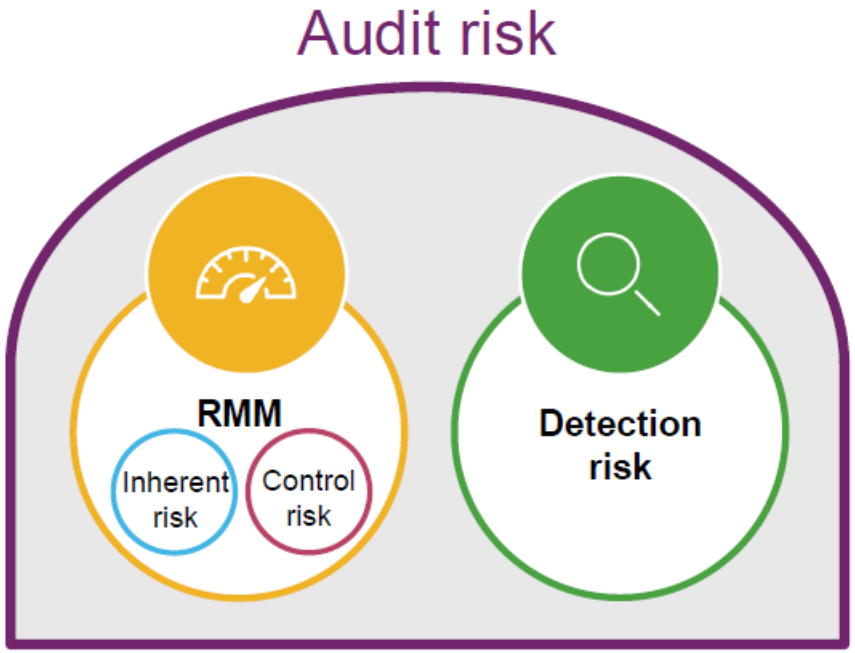
Note that because SAS No. 145 is codified in AU-C section 315, and all AU-C sections are included in *Professional Standards*, from this point the course will refer only to AU-C section 315 as the source of authoritative guidance.

Maner Costerisan

Overview

Audit risk: the risk that we issue an incorrect opinion

Audit risk model



Maner Costerisan

Overview

- Risk assessment
  - Paragraph .13 of AU-C section 315 states that the auditor should design and perform risk assessment procedures to obtain audit evidence that provides an appropriate basis for:
    - The identification and assessment of risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, and
    - The design of further audit procedures in accordance with AU-C section 330

Maner Costerisan

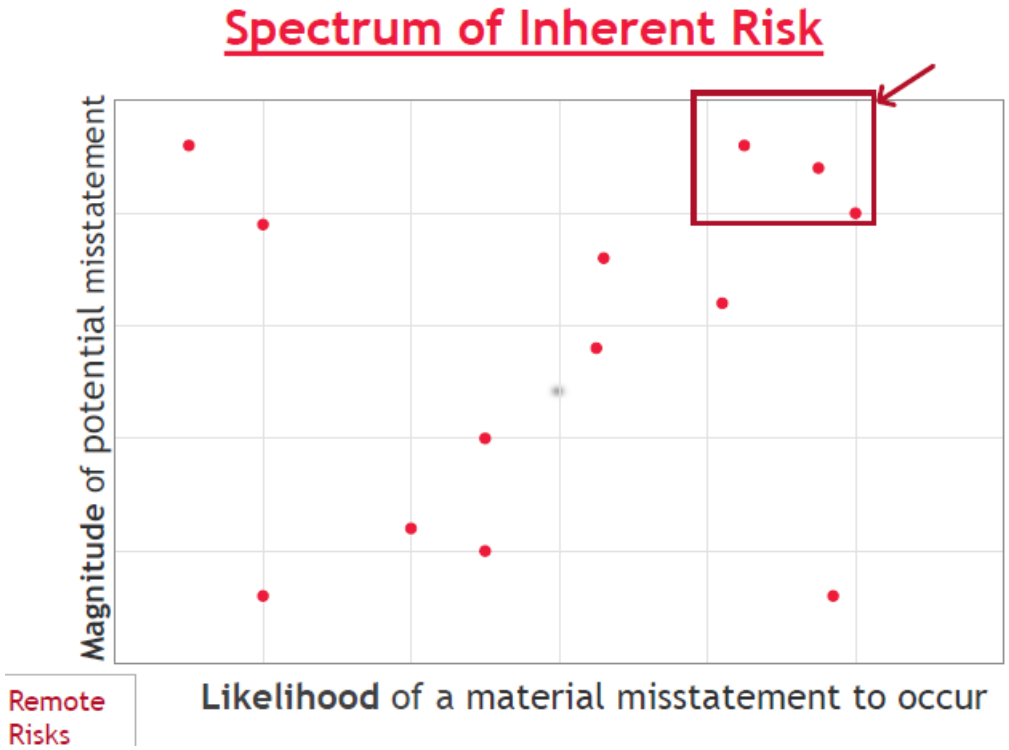
Overview

- Identifying and assessing risk of material misstatement
  - AU-C section 200 requires the auditor to exercise professional judgment in planning and performing an audit
    - This includes planning and performing an audit with professional skepticism
  - For purposes of GAAS, a risk of material misstatement exists when:
    - There is a reasonable possibility of a misstatement occurring
    - If it were to occur, there is a reasonable possibility of the misstatement being material

Maner Costerisan

Overview

Significant risk



Maner Costerisan

Overview

- Identifying and assessing risk of material misstatement
  - Risks reside at the financial statement level or the assertion level (or both)
    - Financial statement level
      - Pervasive (i.e. mgmt. override of controls)
    - Assertion level
      - Relate to one or more relevant assertions in a class of transactions, account balance, or disclosure (i.e. completeness of AP)
    - Both
      - Management override may also relate to assertion-level risks of revenue overstatement

Maner Costerisan

Overview

- Identifying and assessing risk of material misstatement is iterative and dynamic and is interdependent with the following:

Our understanding of the entity and its environment

The applicable financial reporting framework

The entity's system of internal control

Maner Costerisan

Overview

- Assessing risk (AU-C section 315) and performing further audit procedures (AU-C section 330)
  - Clear linkage between identified RMM, the assessment of those risks, and further audit procedures performed in response to the risks
  - AU-C section 315 topped the list for most common MFC-related findings in peer reviews with AU-C section 330 as a close second

Maner Costerisan

Overview

- Risk assessment procedures
  - Paragraph .14 of AU-C section 315 states that the risk assessment procedures should include the following:
    - Inquiries of management and other appropriate individuals
    - Analytical procedures
    - Observation and inspection
  - We are required to perform risk assessment procedures to obtain understanding of the following:
    - The entity and its environment
    - The applicable financial reporting framework
    - The entity's system of internal control

Maner Costerisan

Overview

New and Revised Risk Assessment Terminology and Concepts

- Inherent risk factors
- Spectrum of inherent risk
- Significant class of transactions, account balance, or disclosure
- Relevant assertion and reasonable possibility
- Significant risk

Maner Costerisan

Obtaining an Understanding of the Entity and the Applicable Financial Reporting Framework

Business risk	A risk resulting from significant conditions, events, circumstances, actions, or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies.
Inherent risk factors	Characteristics of events or conditions that affect the susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance, or disclosure, before consideration of controls. Such factors may be qualitative or quantitative and include complexity, subjectivity, change, uncertainty, or susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk.

Maner Costerisan

Obtaining an Understanding of the Entity and the Applicable Financial Reporting Framework

- Inherent risk factors
  - Complexity
    - Nature of the information or the way that the information is prepared
  - Subjectivity
    - Inherent limitations in the ability to prepare information in an objective manner
  - Change
    - Events or conditions that affect the entity's business
  - Uncertainty
    - Arises when it is not possible to prepare financial information based only on sufficiently precise and comprehensive data that is verifiable through direct observation
  - Susceptibility to misstatement due to management bias or other fraud risk factors
    - Incentives or pressures

Maner Costerisan

Obtaining an Understanding of the Entity and the Applicable Financial Reporting Framework

- Paragraph .19 of AU-C section 315 states that we continue risk assessment by performing procedures to obtain an understanding of:
  - The following aspects of the entity and its environment:
    - Organization structure
    - Ownership and governance
    - Business model, including the extent to which it integrates the use of IT
    - Industry, regulatory, and other external factors
    - Measures used, internally and externally, to assess the entity's financial performance
    - The applicable financial reporting framework and the entity's accounting policies and the reasons for any changes
    - How inherent risk factors affect the susceptibility
  - This is our "understanding the entity" form

Maner Costerisan

Obtaining an Understanding of the Entity and the Applicable Financial Reporting Framework

School District Considerations

- Understand ability of the District to make unilateral decisions and ability of other governmental entities to control or influence the District's mandate and strategic direction
- Consider relevant District activities, such as related programs, program objectives and strategies, and public policy elements
- Obtain information from additional resources, such as auditors involved in performance or other audits related to the District
- Inquire of internal audit function about matters related to noncompliance with laws and regulations and control deficiencies
- Consider inspecting documents prepared by management of the District (for example, documents related to performance reporting)

Maner Costerisan

Obtaining an Understanding of the Entity and the Applicable Financial Reporting Framework

School District Considerations

- Budget philosophies
- Debt and investment management
- Primary sources of revenue, such as property taxes, appropriations, and grants
- Federal, state, and local laws and regulations governing the general operations of the District and its component units
- Factors affecting the continued functioning of the District, such as the presence or absence of taxpayer initiatives that limit its budget growth or addition of services

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

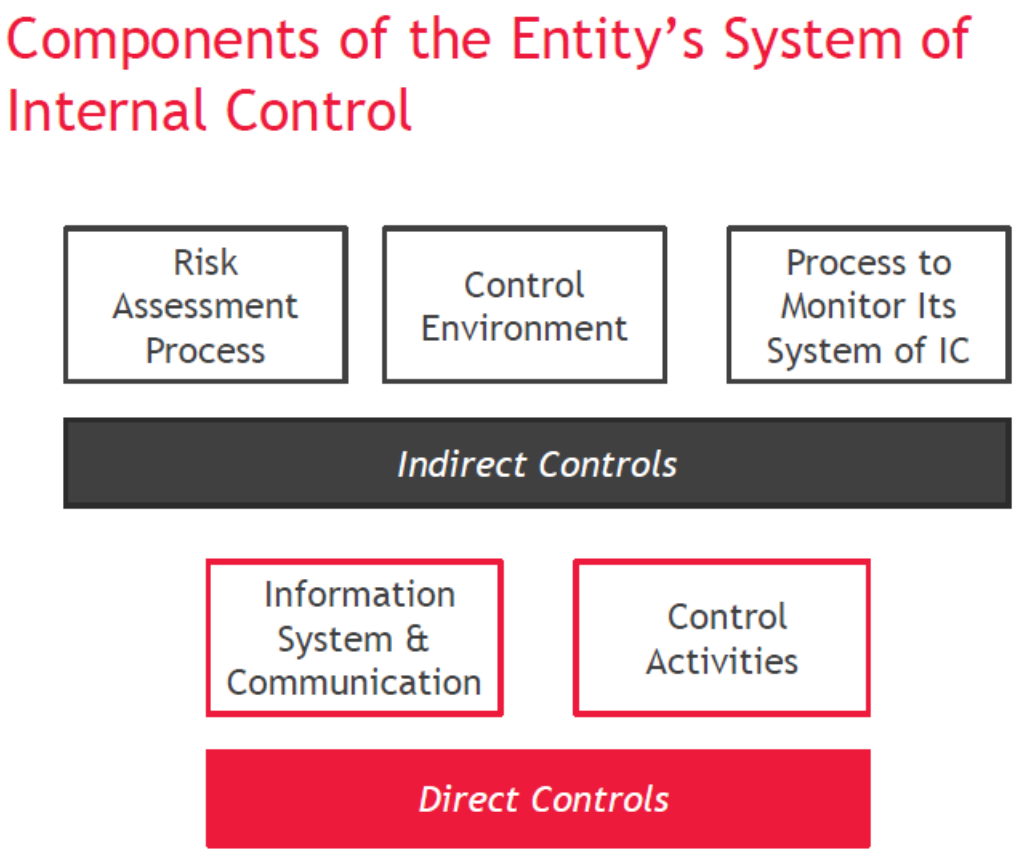
What is a system of internal control?

A **system of internal control** is

- maintained by the entity
- to provide reasonable assurance about
  - reliability of financial reporting,
  - effectiveness and efficiency of operations, and
  - compliance with applicable laws and regulations.

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control



Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Information System & Communication

For the entity's information system and communication, we are required to

understand the flows of transactions and other aspects of the entity's information-processing activities relevant to the preparation of the financial statements

evaluate whether the component appropriately supports the preparation of the entity's financial statements

  - Doing so supports our identification and assessment of risks of material misstatement at the assertion level
- Control Activities
  - Required to identify specific controls, evaluate the design, and determine whether the controls have been implemented

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Purpose of understanding the components
  - Assists in developing initial expectations about various items such as classes of transactions, account balances, and disclosures that may be significant
  - Expectations can be used to determine the extent of understanding of the entity's information-processing activities to be obtained
- Inherent risk
  - Our assessment of inherent risk may influence the identification of controls in the control activities component
  - Remember, the higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence must be
  - If not testing controls, then IR = RMM

Even when the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still affect the design of the nature, timing, and extent of AU-C section 330 substantive procedures that are responsive to the related risks of material misstatement.

It is important to remember that our identification and assessment of risks of material misstatement at the assertion level is influenced by both

- our understanding of the entity's policies for its information-processing activities in the information system and communication component, and
- our identification and evaluation of controls in the control activities component.

Maner Costerisan

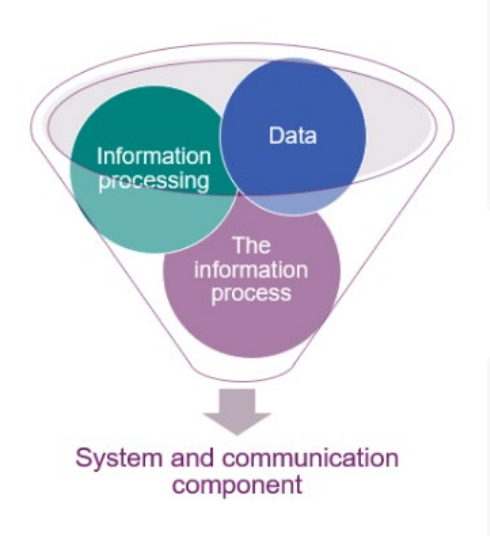
Obtaining an Understanding of the Entity's System of Internal Control

- Information System and Communication
  - We fulfill this requirement by understanding the following:
    - The entity's information-processing activities, including its data and information
      - The resources to be used in such activities
      - The policies that define how information flows through the entity's information system for significant classes of transactions, account balances, and disclosures
  - What are we talking about? WALKTHROUGHS

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Information System and Communication
  - Understanding risks to the integrity of the information system include the following:
    - The competence of the individuals undertaking the work
    - Whether there are adequate resources
    - Whether there is appropriate segregation of duties
  - Matters to consider when understanding the policies that define the flows of information include:
    - The data or information relating to transactions, other events, and conditions to be processed
    - The information processing to maintain the integrity of that data or information
    - The information processes, personnel, and other resources used in processing information
  - How do we obtain the understanding?
    - Inquiries
    - Inspection
    - Observation
    - Selecting transactions and performing a walkthrough



Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Information System and Communication
  - The IT environment relevant to the information system
    - Focus on identifying and understanding the nature and number of specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system
    - This may help to identify any risks arising from the use of IT
    - This should be documented on an IT environment form and perhaps a separate IT General Controls form
  - Remember scalability
    - Even in a less complex entity, which may require less effort to understand the IT environment, it is still required
- Communication
  - Should perform risk assessment procedures to understand how an entity communicates significant matters that support the preparation of the financial statements

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Information System and Communication
  - Once we understand the information system and communication, we should complete an evaluation
    - This should be documented

Controls within the information system and communication component are primarily more direct in addressing assertion level risks but may also be indirect (see paragraphs .A5, .A105, and .A140 of AU-C section 315). In particular, information-processing controls, also known as transaction controls, directly support the actions to mitigate information-processing risks in an entity's business processes (see paragraphs .A7–.A8).

As described in paragraph .A169, although the auditor's identification and evaluation of controls in the control activities component as required by paragraph .30 is focused on information-processing controls, the auditor is not required to identify and evaluate all information-processing controls related to the entity's policies that define the flows of transactions and other aspects of the entity's information-processing activities for the significant classes of transactions, account balances, and disclosures.

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Understanding the entity's control activities component requires us to do the following:
  - Identify the controls that address risks of misstatement at the assertion level
  - Identify any IT applications used or other aspects of IT that may create risk
  - Identify risks arising from the use of IT and the controls that address them
  - Evaluate the design and implementation of identified controls in the control activities component

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Required to identify the controls that address risks of misstatement at the assertion level:
  - Controls that address a risk that is determined to be significant
    - Presumed significant risks: management override of controls, revenue recognition, and related party transactions that are significant unusual transactions
    - Also consider nonroutine events not subject to routine controls and management's responses intended to deal with these risks
  - Controls over journal entries and other adjustments as required by AU-C section 240
    - Controls related to assessed risks of material misstatement due to fraud (i.e. management override of controls)
  - Controls for which the auditor plans to test operating effectiveness
    - Generally we do not test controls in a financial statement audit
  - Other controls that, based on auditor's professional judgement, the auditor considers are appropriate to enable the auditor to meet the objectives with respect to risks at the assertion level
    - Controls that address risks assessed as higher on the spectrum of inherent risk but have not been determined to be a significant risk
    - Controls related to reconciling detailed records to the general ledger
    - Controls related to accounting estimates
    - Complementary user entity controls, if using a service organization
- Not required to identify and evaluate all controls related to each significant transaction class
  - Only the key controls

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Identify any IT applications used or other aspects of IT that may create risk
  - Based on the relevant controls identified in the 4 categories on the previous slide, we should identify the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT
  - For the IT applications and other aspects of the IT environment identified, we should further identify the related risks arising from the use of IT, and the entity's general IT controls that address such risks
  - These should be documented
- While we are required to obtain an understanding and identify risks, as noted above, we generally assess control risk at high already which then calls for related risks arising from the use of IT to be addressed through the design of substantive procedures

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Identify risks arising from the use of IT and the controls that address them
  - Primarily unauthorized access or unauthorized program changes as well as risks related to inappropriate data changes
  - Consider whether there is a risk when an entity uses external service providers for their IT environment
  - Consider risks related to cybersecurity
  - Scalability – when volume or complexity of automated application controls is higher, and management is placing greater reliance on those controls for effective processing of transactions, there may be more risk

Maner Costerisan

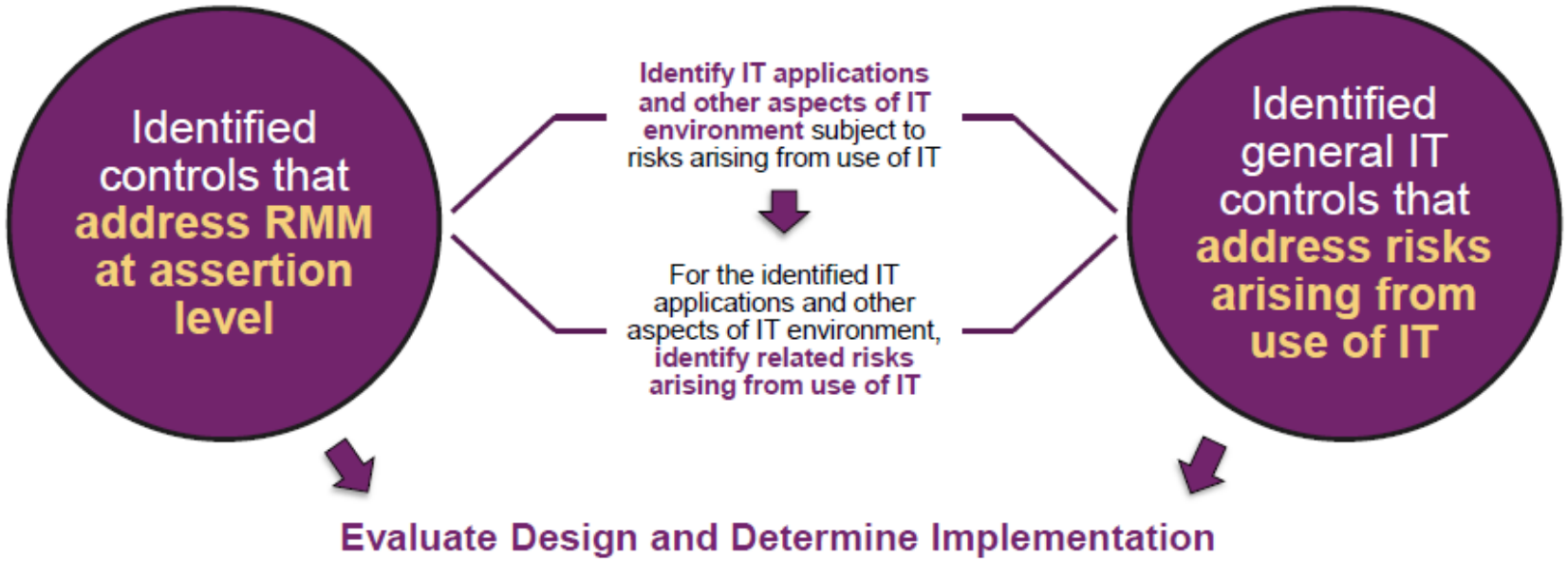
Obtaining an Understanding of the Entity's System of Internal Control

- Risks arising from the use of IT
  - Susceptibility of information-processing controls to ineffective design or operation, or risks to the integrity of information in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes
  - Consider risks related to:
    - How the entity manages access, including privileged access
    - How the entity manages program or other changes
    - How the entity manages IT operations, including batch or job scheduling

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

General IT Controls



Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

General IT Controls

Examples of the Types of IT Systems or Applications and Related Considerations

Software as a service (third party hosting or outsourcing)

- Is a service organization control report available?
- Are controls configurable by the user entity? Has the entity implemented complementary user entity controls over changes to configurations?

Purchased systems or applications

- Are changes limited to patches, updates, and minor configurations?
- If configurable, who can customize changes (the entity or vendor)?

Internally developed systems or applications

- What types of changes were made during the period?
- Who has access to source code?

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

General IT Controls

Examples of Risks Arising from the Use of IT

IT Process	Examples of Risks Arising from Use of IT	IT Considerations
Manage access	• Users have access privileges beyond those necessary to perform assigned duties • Systems are not adequately configured or updated to restrict system access • Inappropriate changes are made through direct data access	• IT application layer authentication • Technical security configurations • System-enabled segregation
Manage program or other changes	• Inappropriate changes are made to system software, application systems, or the database structure • Data converted from legacy systems or previous versions introduce data errors	• Access to source code • Ability to change databases
Manage IT operations	• Network does not adequately prevent unauthorized users from gaining access • Production systems, programs, or jobs result in inaccurate, incomplete, or unauthorized processing of data • Financial data cannot be recovered in a timely manner when there is a loss of data	• Network authentication methods • Batch processing

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

General IT Controls

Examples of General IT Controls

IT Process	Examples of General IT Controls
Manage access	• Authentication • Authorization • Provisioning • Deprovisioning • Privileged access • User-access reviews • Security configuration controls • Physical access
Manage program or other changes	• Change-management • Segregation of duties over change migration • Systems development or acquisition or implementation • Data conversion
Manage IT operations	• Job scheduling • Job monitoring • Backup and recovery • Intrusion detection

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

- Evaluate the design and implementation of identified controls in the control activities component
  - Auditors should evaluate each control identified in the four categories, or for the entity's general IT controls
  - These are our walkthroughs
  - Focus on key controls and the relevant assertions that each control addresses
  - Is the control, individually or in combination with other controls, capable of effectively preventing, or detecting and correcting, material misstatements?
    - If the answer is no, we may have a control deficiency
  - Evaluate the design of the control first and then determine whether it was implemented effectively by:
    - Inquiring of entity personnel
    - Observing the performance of the control
    - Inspecting documents and reports
    - Reperforming the control
  - Documentation is required

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

School District Considerations

- Information processing activities:
  - Investments and equity interests
  - Revenues and receivables
  - Capital assets
  - Expenses or expenditures
  - Interfund, internal, and intra-entity activities
- Generally, the focus is on information coming out of the general ledger
  - Munis, School Finance, Skyward, Smart
- What about other systems?
  - POS systems (Meal Magic, athletics, student activities)

Maner Costerisan

Obtaining an Understanding of the Entity's System of Internal Control

School District Considerations

- We will need the help of the IT team
  - Start this process during preliminary fieldwork
  - Determine what systems are involved in the preparation of the financial statements
  - Determine if there are risks arising from the use of IT within those systems
  - Determine the controls that are in-place to address the risks
  - Evaluate design and implementation of the identified key controls

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Useful definitions

Assertions[1]	Representations, explicit or otherwise, with respect to the recognition, measurement, presentation, and disclosure of information in the financial statements, which are inherent in management, representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing, and responding to the RMMs.
Significant class of transactions, account balance, or disclosure[2]	A class of transactions, account balance, or disclosure for which there is one or more relevant assertions.
Significant risk	An identified RMM i. 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 ii. that is to be treated as a significant risk in accordance with the requirements of other AU-C sections.

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- AU-C section 315 tells us that the auditor should identify the RMMs and determine whether they exist in two areas:
  - The financial statement level
  - The assertion level for classes of transactions, account balances, or disclosures
- The identification of RMMs is performed before consideration of any related controls
  - In other words, it is based on inherent risk
  - It is based on our preliminary consideration of misstatements that have a reasonable possibility of both occurring and being material if they were to occur

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Identifying and assessing RMMs at the financial statement level
  - Required in order to determine whether the risks have a pervasive effect on the financial statements
    - May also affect individual assertions
  - Influenced by our understanding of the three indirect controls
    - The control environment
    - The entity's risk assessment process
    - The entity's process to monitor the system of internal control
  - Also influenced by control deficiencies identified in the control environment
    - For example, lack of management competence or oversight over the preparation and fair presentation of the financial statements
  - Fraud or suspected fraud should also be considered here
    - i.e. Management override of control

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Identifying and assessing RMMs at the assertion level
  - Assessed at the assertion level in order to determine the nature, timing, and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence
- For identified RMMs at the assertion level, the auditor should assess inherent risk by determining the likelihood and magnitude of misstatement
  - Low, moderate, high (or not relevant)
  - The higher the risk, the more significant the risk is, and the more persuasive audit evidence is required
- For identified risks that are significant, required responses include:
  - Controls that address significant risks are required to be identified, with a requirement to evaluate whether the control has been designed effectively and implemented
  - Controls that address significant risks are required to be tested when the auditor plans to rely on their operating effectiveness
  - Substantive procedures are to be planned and performed that are specifically responsive to the identified significant risk
  - Required to communicate significant risks to those charged with governance

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Identifying and assessing RMMs at the assertion level

RMMs that may be assessed as having higher inherent risk and which therefore may be determined to be a significant risk may arise from matters such as the following:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved
- Accounting estimates that have high estimation uncertainty or complex models
- Accounting for unusual or complex transactions, for example, accounting for revenue with multiple performance obligations that are difficult to value
- Emerging areas, for example, accounting for digital assets
- Complexity in data collection and processing to support account balances
- Account balances or quantitative disclosures that involve complex calculations
- Accounting principles that may be subject to differing interpretation
- Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions.

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Completing Risk Assessment Procedures
  - Evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the RMMs
  - Remember professional skepticism – is there any contradictory evidence to consider as well?
  - For material classes of transactions, account balances, or disclosures that have not been determined to be significant, the auditor should evaluate whether the determination remains appropriate
  - If necessary, revise the risk assessment. Remember it is dynamic and iterative.

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

- Linking risk assessment to further audit procedures
  - The auditor should perform substantive procedures for each relevant assertion of each significant class of transactions, account balance, and disclosure
  - If we have determined that an assessed RMM at the relevant assertion level is a significant risk, we should perform substantive procedures that are specifically responsive to that risk
  - When the approach to the significant risk consists only of substantive procedures, those procedures should include tests of details
  - Consider utilizing the comments section of each audit area in the risk assessment form to provide details linking risk assessments to further audit procedures

Maner Costerisan

Identifying and Assessing the Risks of Material Misstatement and Further Audit Procedures

School District Considerations

- Significant risks identified should be communicated to those charged with governance
  - How will the board respond?
- Has anything happened during FY-24 (or after year-end) that could be considered a new risk or a heightened risk?
  - Turnover in key personnel
  - Fraud
  - NOCLAR
  - Budgets
  - Change in systems
  - Change in internal controls

Maner Costerisan

Key Takeaways

- Risk assessment concepts are principles based, methodology agnostic, and scalable; risk assessment is a dynamic and iterative process
- New and revised risk assessment terminology and concepts, including significant risks
- Clarified work effort related to understanding each of the components of internal control, including enhanced guidance on IT
- Several new requirements:
  - Separately assess inherent risk and control risk
  - “Maximum” control risk when controls are not tested for operating effectiveness
  - Risk assessment “stand-back”

Maner Costerisan

State and Local Governments A&A Guide

- Includes both pre-SAS 145 and post-SAS 145 guidance
- Chapter 4 revisions:
  - Five new inherent risk factors: subjectivity, complexity, uncertainty, change and susceptibility to misstatement due to management bias or fraud
  - Requires separate assessments of inherent and control risk
  - If no tests of controls are performed, RMM = Inherent Risk
  - Requires “sufficient, appropriate” evidence as basis for risk assessment
  - Stand-back requirement for material classes of transactions, account balances, or disclosures not assessed as significant

Maner Costerisan

Compliance Audits

Reminders, Clarifications, and Changes

- The concept of significant risk does not apply
- Identified controls for which the auditor evaluates design and determines implementation differ from financial statement audit
  - Do not include controls over significant risks
  - Include controls required to be tested for operating effectiveness by the governmental audit requirement
- Inherent risk and control risk are assessed for each applicable compliance requirement
  - Inherent risk takes into account inherent risk factors
  - Remember we are required to design our audit procedures to support a low assessed level of control risk of noncompliance
- Document identified and assessed risks and rationale for significant judgments
- Sample sizes may change depending on how populations are defined and how we risk assess each direct and material compliance requirement

Maner Costerisan

Questions?

Maner Costerisan

Thank you

Contact Information
Dave Nielsen: dnielsen@manercpa.com
Nick West: nwest@manercpa.com

Maner Costerisan