Rehmann *Live!*

The New COSO: Internal Control - Integrated Framework

September 17, 2014

Webinar

Presented in association with AGA

AGA

Rehmann

Presented by:

Stephen W. Blann, CPA, CGFM, CGMA
Director of Governmental Audit Quality
Rehmann

Session Outline

- Defining internal control
- Objectives, components, and principles
- Limitations on internal control
- Deficiencies in internal control
- Internal control over compliance
- Considerations for smaller entities

Overview of Internal Control

- Internal Control—Integrated Framework
  - COSO Report (1992 & 2013)
  - Committee of Sponsoring Organizations (AICPA, AAA, IIA, IMA, FEI)
  - Codified in Auditing Standards by AICPA, GAO, OMB, and PCAOB (SOX)

Defining Internal Control

- Internal control is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance

Defining Internal Control

- Internal control is:
  - *Geared to the achievement of objectives* in one or more separate but overlapping categories:
    - Operations
    - Reporting
    - Compliance

Defining Internal Control

- Internal control is:
  - *A process* consisting of ongoing tasks and activities—a means to an end, not an end in itself

Defining Internal Control

- Internal control is:
  - *Effected by people*—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control

Defining Internal Control

- Internal control is:
  - Able to *provide reasonable assurance*—but not absolute assurance, to an entity's senior management and board of directors

Defining Internal Control

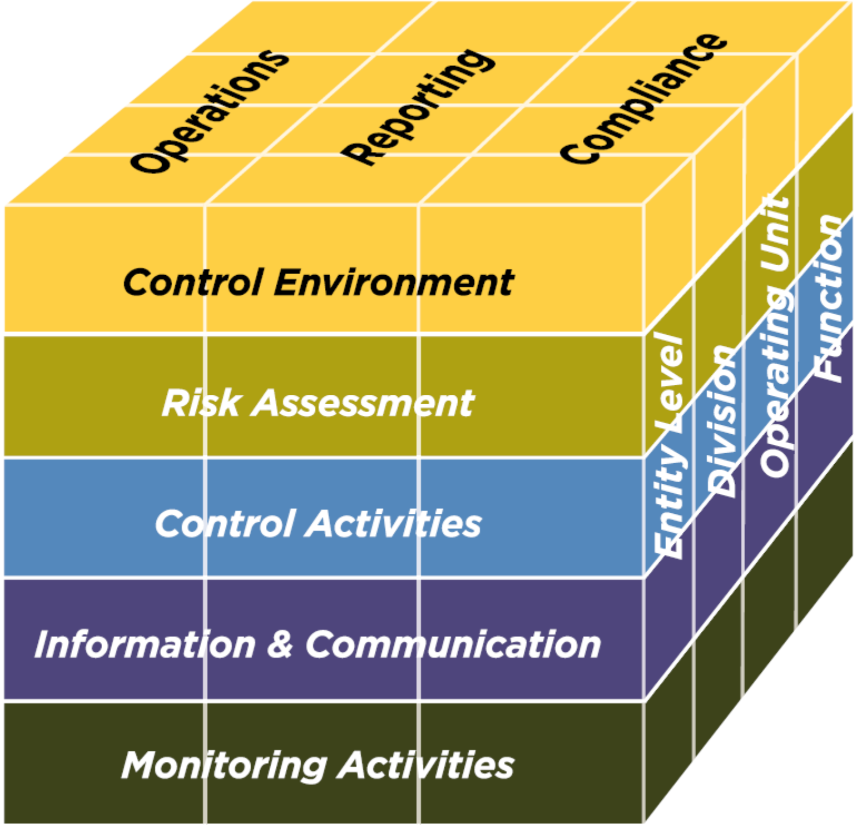
- Internal control is:
  - *Adaptable to the entity structure*—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

Objectives, Components, & Principles

- Objectives:
  - Operations, reporting, compliance
- Components:
  - Control environment, risk assessment, control activities, information/communication, monitoring
- Principles:
  - 17 concepts applicable to the 5 components

Objectives, Components, & Principles

- Each principle and component is applicable to each objective at each level of an organization



Objectives

- Operations objectives:
  - Achievement of the entity's basic mission and vision (effectiveness)
  - Safeguarding of assets (preservation and efficiency)

Objectives

- Reporting objectives:
  - External vs. internal
  - Financial vs. non-financial

Objectives

- Compliance objectives:
  - Laws and regulations
  - Provisions of grant agreements

Components and Principles

Control Environment

- The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization

Components and Principles

Control Environment

- **Principle 1: Demonstrates Commitment to Integrity and Ethical Values**
  The organization demonstrates a commitment to integrity and ethical values.
  - Sets the Tone at the Top
  - Establishes Standards of Conduct
  - Evaluates Adherence to Standards of Conduct
  - Addresses Deviations in a Timely Manner

Components and Principles

Control Environment

- **Principle 2: Exercises Oversight Responsibility** The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
  - Establishes Oversight Responsibilities
  - Applies Relevant Expertise
  - Operates Independently
  - Provides Oversight for the System of Internal Control

Components and Principles

Control Environment

- **Principle 3: Establishes Structure, Authority, and Responsibility**
  Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
  - Considers All Structures of the Entity
  - Establishes Reporting Lines
  - Defines, Assigns, and Limits Authorities and Responsibilities

Components and Principles

Control Environment

- **Principle 4: Demonstrates Commitment to Competence**
  The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
  - Establishes Policies and Practices
  - Evaluates Competence and Addresses Shortcomings
  - Attracts, Develops, and Retains Individuals
  - Plans and Prepares for Succession

Components and Principles

Control Environment

- **Principle 5: Enforces Accountability**
  The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
  - Enforces Accountability
  - Establishes Performance Measures, Incentives, and Rewards
  - Evaluates Measures, Incentives, and Rewards for Ongoing Relevance
  - Considers Excessive Pressures
  - Evaluates Performance and Rewards or Disciplines Individuals

Components and Principles

Risk Assessment

- A dynamic and iterative process for identifying and assessing the possibility that an event will occur and adversely affect the achievement of objectives

Risk Assessment

- **Principle 6: Specifies Suitable Objectives** The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
  - Reflects Management's Choices
  - Considers Tolerances for Risk
  - Includes Operations and Financial Performance Goals
  - Forms a Basis for Committing of Resources
  - Complies with reporting/compliance frameworks

Components and Principles

Risk Assessment

- **Principle 7: Identifies and Analyzes Risk**
  The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
  - Includes Entity, Subsidiary, Division, Operating Unit, & Functional Levels
  - Analyzes Internal and External Factors
  - Involves Appropriate Levels of Management
  - Estimates Significance of Risks Identified
  - Determines How to Respond to Risks

Components and Principles

Risk Assessment

- **Principle 8: Assesses Fraud Risk**
  The organization considers the potential for fraud in assessing risks to the achievement of objectives.
  - Considers Various Types of Fraud
  - Assesses Incentive and Pressures
  - Assesses Opportunities
  - Assesses Attitudes and Rationalizations

Components and Principles
Risk Assessment

- **Principle 9: Identifies and Analyzes Significant Change**
  The organization identifies and assesses changes that could significantly impact the system of internal control.
  - Assesses Changes in the External Environment
  - Assesses Changes in the Business Model
  - Assesses Changes in Leadership

Components and Principles

Control Activities

- The actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out

Components and Principles

Control Activities

- **Principle 10: Selects/Develops Control Activities** The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
  - Integrates with Risk Assessment
  - Considers Entity-Specific Factors
  - Determines Relevant Business Processes
  - Evaluates a Mix of Control Activity Types
  - Considers at What Level Activities Are Applied
  - Addresses Segregation of Duties

Components and Principles

Control Activities

- **Principle 11: Selects and Develops General Controls over Technology**
  The organization selects and develops general control activities over technology to support the achievement of objectives.
  - Determines Dependency between the Use of Technology in Business Processes and Technology General Controls
  - Establishes Relevant Technology Infrastructure Control Activities
  - Establishes Relevant Security Management Process Control Activities
  - Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities

Components and Principles

Control Activities

- **Principle 12: Deploys Policies and Procedures** The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Components and Principles

Information and Communication

- The continual, iterative process of providing, sharing, and obtaining necessary information to carry out internal control responsibilities to support the achievement of the entity's objectives

Components and Principles

Information and Communication

- **Principle 13: Uses Relevant Information** The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
  - Identifies Information Requirements
  - Captures Internal and External Sources of Data
  - Processes Relevant Data into Information
  - Maintains Quality throughout Processing
  - Considers Costs and Benefits

Components and Principles

Information and Communication

- **Principle 14: Communicates Internally**
  The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
  - Communicates Internal Control Information
  - Communicates with the Board of Directors
  - Provides Separate Communication Lines
  - Selects Relevant Method of Communication

Components and Principles

Information and Communication

- **Principle 15: Communicates Externally**
  The organization communicates with external parties regarding matters affecting the functioning of internal control.
  - Communicates to External Parties
  - Enables Inbound Communications
  - Communicates with the Board of Directors
  - Provides Separate Communication Lines
  - Selects Relevant Method of Communication

Components and Principles

Monitoring Activities

- Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning

Components and Principles

Monitoring Activities

- **Principle 16: Conducts Ongoing / Separate Evaluations** The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
  - Considers a Mix of Ongoing and Separate Evaluations
  - Considers Rate of Change
  - Establishes Baseline Understanding
  - Uses Knowledgeable Personnel
  - Integrates with Business Processes
  - Adjusts Scope and Frequency
  - Objectively Evaluates

Components and Principles

Monitoring Activities

- **Principle 17: Evaluates and Communicates Deficiencies**
  The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
  - Assesses Results
  - Communicates Deficiencies
  - Monitors Corrective Actions

Limitations of Internal Control

- Internal control, no matter how well designed, implemented and conducted, can provide only *reasonable assurance* to management and the board of directors of the achievement of an entity's objectives.

Limitations of Internal Control

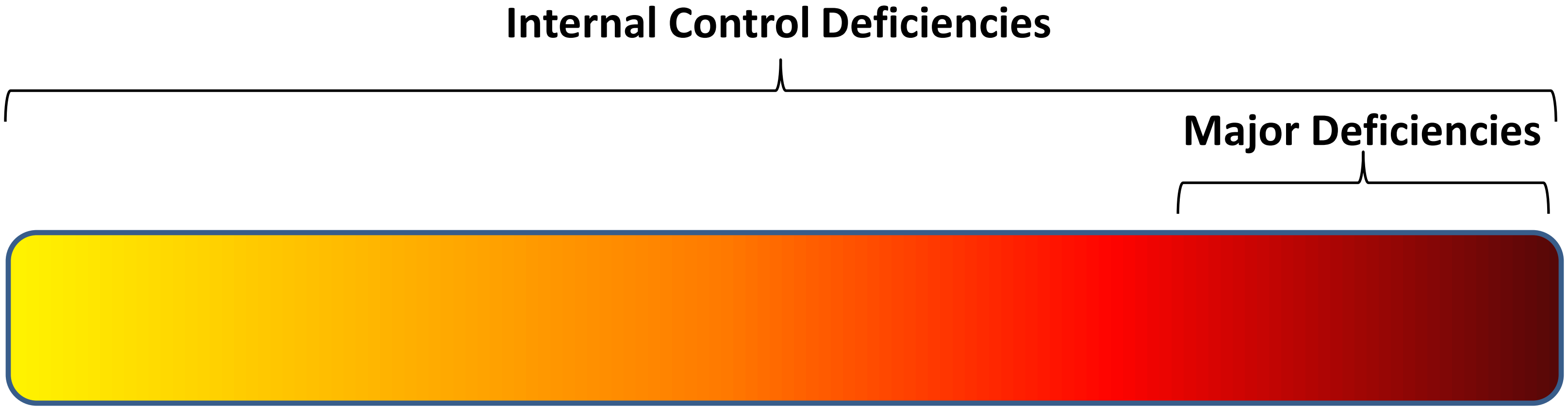
- Judgment
- External events
- Breakdowns
- Management override
- Collusion

Deficiencies in Internal Control

- Internal control deficiency
  - a shortcoming in a component or components and relevant principle(s) that reduces the likelihood of an entity achieving its objectives
- Major deficiency
  - an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives

Deficiencies in Internal Control

- Assessing severity



Deficiencies in Internal Control

- Responding to identified deficiencies
  - Consider the control environment
  - Assess risks
  - Establish/revise policies and procedures
  - Communicate changes
  - Monitor results

Internal Control over Compliance

- Differences and similarities with IC over financial reporting
- Existing and new requirements for grants
- Auditor involvement / testing

Internal Control over Compliance

- Existing grant requirements:
  - OMB Circulars A-102 Common Rule and A-110 Administrative Requirements
  - Requires management to establish and maintain internal controls designed to provide reasonable assurance of compliance with Federal laws, regulations and program compliance requirements

Internal Control over Compliance

- New Uniform Grant Guidance (2 CFR 200):
  - Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award
  - Follow COSO's Integrated Framework
  - Include written procedures

Internal Control over Compliance

- Auditor involvement / testing
  - Yellow Book engagements (material to financial statements)
  - Single audit (material to major federal programs)
  - Other (Medicare, etc.)

Considerations for Smaller Entities

COSO – One Size Fits All?

- In 2006, COSO issued a tailored version of its 1992 report, entitled Guidance for Smaller Public Companies (now in Appendix C)
- Not specifically targeted at governments, but helpful nonetheless
- Emphasizes the cost vs. benefit principle of internal control

Considerations for Smaller Entities

Cost vs. Benefit

- Entities always have limits on human and capital resources and constraints on how much they can spend, and therefore they will often consider the costs relative to the benefits of alternative approaches in managing internal control options
  - Cost alone is not an acceptable reason to avoid implementing internal control

Considerations for Smaller Entities

“Small” vs. “Smaller”

- There is no “bright line” to define governments as small, medium-size or large
  - Fewer types of services provided
  - Fewer personnel, many having a wider range of duties
  - Fewer levels of management, with wider spans of control
  - Less complex transaction processing systems and protocols

Challenges for Smaller Governments

- Maintaining cost-effective internal control:
  - Managers that view internal control as a burden, rather than a benefit
  - Obtaining sufficient resources for adequate segregation of duties
  - Management's ability to dominate activities and override internal control
  - Recruiting/retaining personnel with sufficient experience and skill in financial reporting and/or computer information systems

Challenges for Smaller Governments

- Potential solutions:
  - Wide and direct control from the top
  - Effective governing bodies
  - Compensating for limited segregation of duties
  - Information technology
  - Monitoring activities

Considerations for Smaller Entities

Control from the Top

- Smaller governments may have one or more members of senior management that have an in-depth understanding of virtually all of the government’s operations
  - Can enhance effectiveness of internal control
  - Enables leaders to know what to expect and follow up on differences
  - Adds to risk of management override

Considerations for Smaller Entities

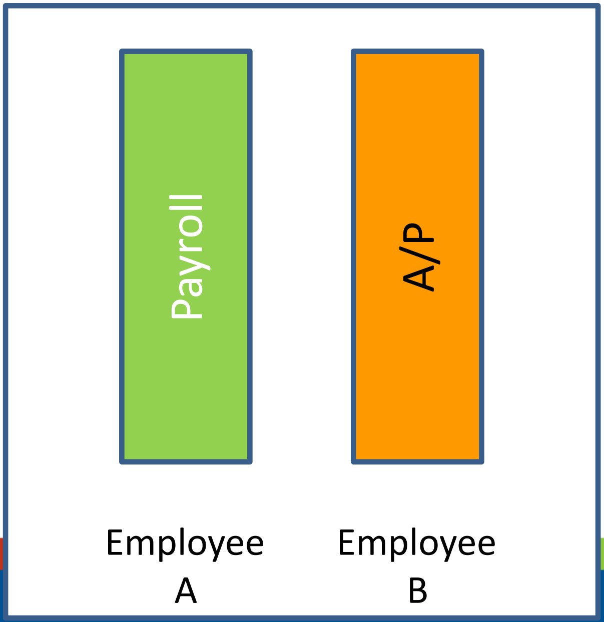
Effective Governing Bodies

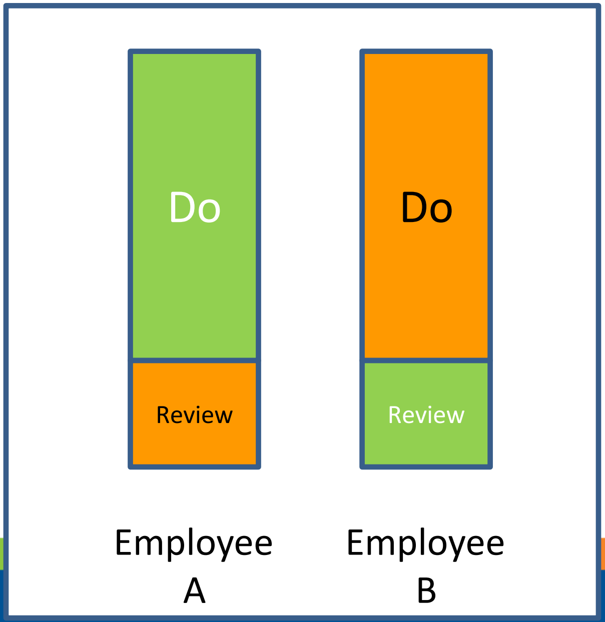
- Smaller governments have less complex structures, and may have more involved boards
  - Direct exposure to management
  - Careful review of monthly reporting, with follow-up questions
  - Extensive public transparency

Considerations for Smaller Entities

Compensating for Limited SoD

- When it isn’t practical to fully segregate all duties, introduce supervision and review
  - Two sets of eyes are better than one





Considerations for Smaller Entities

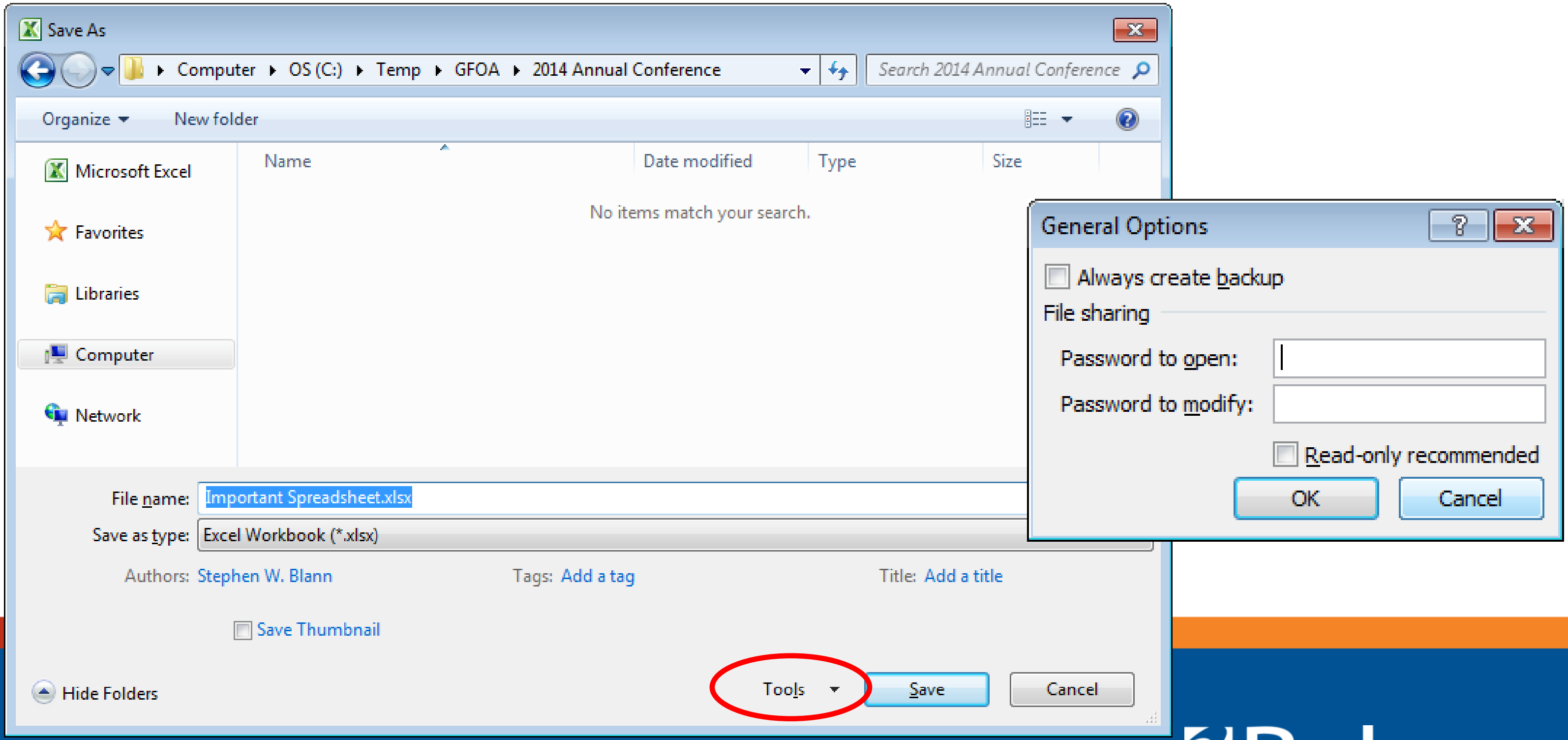
Information Technology

- Smaller governments tend to rely on “off-the-shelf” software
  - Not risk-free, but lower risk
  - Built-in features for limiting access
  - Be sure to use audit-trails, flags, and exception reports if available

Considerations for Smaller Entities

Information Technology

- Securing important spreadsheets from accidental or unauthorized changes



File name: Important Spreadsheet.xlsx

Save as type: Excel Workbook (*.xlsx)

Authors: Stephen W. Blann

Tags: Add a tag

Title: Add a title

□ Save Thumbnail

General Options

□ Always create backup

File sharing

Password to open:

Password to modify:

□ Read-only recommended

Considerations for Smaller Entities

Monitoring Activities

- Monitoring is an important part of the COSO Framework.
  - Management of smaller governments regularly perform such procedures, but have not always taken sufficient “credit” for their contribution to internal control effectiveness
  - Usually performed manually, but may rely on technology

Considerations for Smaller Entities

Controls vs. Processes

- It is easy to confuse the processes used to create transactions with the controls designed to prevent or detect errors in those transactions
- Smaller governments frequently use IT systems to process financial transactions, but design manual controls to review the output of those systems

Considerations for Smaller Entities

Automated vs. Manual Controls

- Generally Accepted Auditing Standards (GAAS) recognize the difference between automated and manual controls (AU-C 315.A53)
  - Manual controls may be independent of IT or may use information produced by IT
  - Smaller governments may need to rely more heavily on manual controls in the absence of a comprehensive set of IT controls

Considerations for Smaller Entities

Achieving Further Efficiencies

- Controls should focus on financial reporting objectives directly applicable to the government’s activities and services:
  - Risk-based approach to internal control
  - Right-sizing documentation
  - Viewing internal control as an integrated process

Considerations for Smaller Entities

Focusing on Risk

- Risk-based controls focus on quantitative and qualitative factors that potentially impact the reliability of financial reporting
  - Identify transactions or processes where something could go wrong
  - Assess likelihood and significance
  - Design controls specifically tailored to those risks
  - Don’t rely on generic controls designed for “typical” governments without modification

Considerations for Smaller Entities

Right-Sizing Documentation

red·tape ***noun***

: excessive regulation or rigid conformity to formal rules that is considered redundant or bureaucratic and hinders or prevents action or decision-making

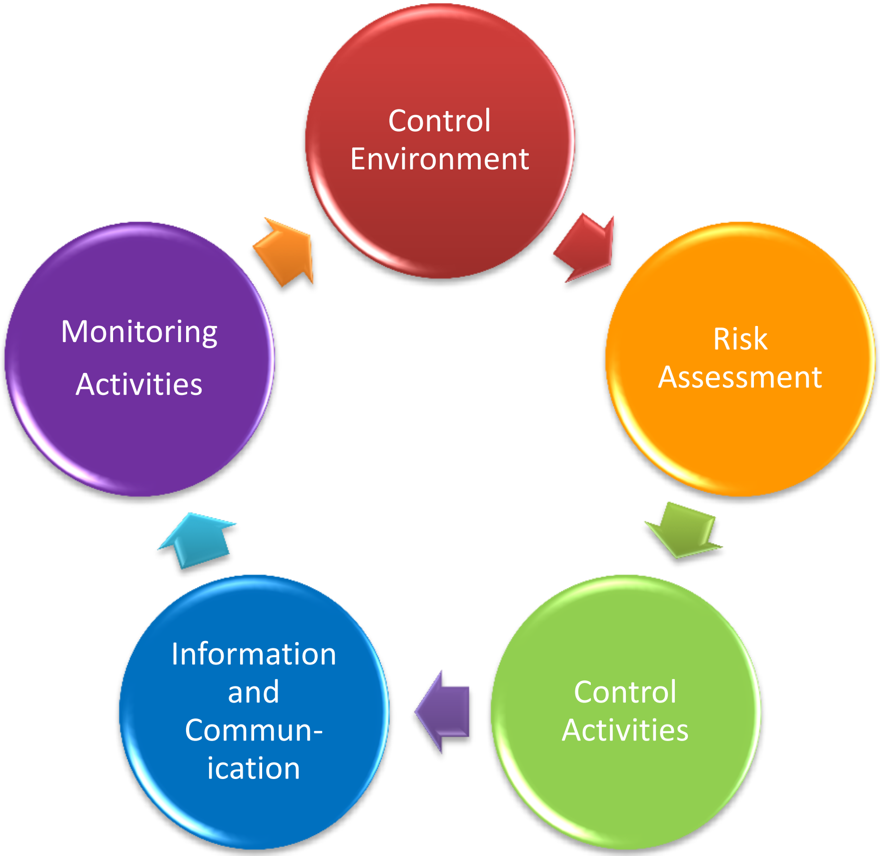
Considerations for Smaller Entities

Right-Sizing Documentation

- Smaller governments should determine the nature and extent of their documentation needs
  - Promote consistency
  - Provide evidence of control effectiveness
  - While smaller governments may not require as formal documentation, certain elements (such as risk assessment) cannot be performed entirely in the CFO’s head

Considerations for Smaller Entities

Viewing IC as an Integrated Process



- Remember the interrelationship of the 5 elements
  - Management has flexibility in choosing controls
  - Should adjust and improve controls over time
  - Effectiveness is measured overall, not by element

Considerations for Smaller Entities

Final Thoughts

- Remember the objective of internal control
- Design controls that are consistent with the government's risk assessment and resources
- Mitigate deficiencies in internal control with as much supervision and review as possible
  - Management
  - Governing body
  - Others within the organization

Questions?

For more information…

Rehmann
Business wisdom delivered.
CPAs & Consultants • Wealth Advisors • Corporate Investigation

Stephen W. Blann, CPA, CGFM, CGMA
Director of Governmental Audit Quality
Rehmann
stephen.blann@rehmann.com
www.rehmann.com/government