



## The North Carolina Office of the State Controller

### Internal Controls: Design for Risk Webinar April 24, 2013

**David McCoy**  
**State Controller**



### Learning Objectives

- Understanding the basics of internal controls
  - Internal Control – Definition and Objectives
  - Fundamental Concepts
- The COSO framework practical application
  - The Control environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring



## Internal Control – Definition and Objectives

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission provides the commonly accepted definition and framework for Internal Controls.

### Internal Control

An integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Management has a fundamental responsibility to develop and maintain effective internal control.

3



## Internal Control – Fundamental Concepts

### Internal Control

- ***Is a continuous built-in component of operations:*** Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis.
- ***Is effected by people.*** People are what make internal control work.
- ***Provides reasonable assurance, not absolute assurance.*** No matter how well designed and operated, internal control cannot provide absolute assurance that all objectives will be met.

4



## The COSO Framework Explained

Internal control consists of five interrelated components.

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information & Communication
5. Monitoring

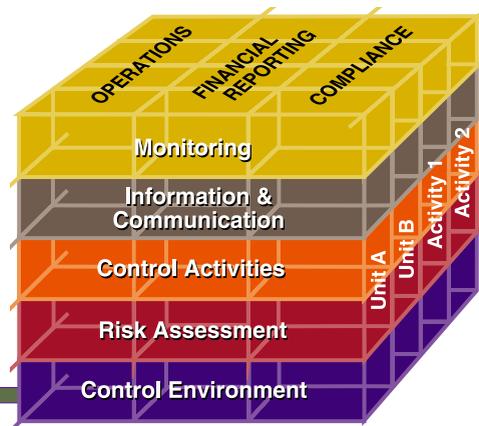


These are derived from the way management runs its business and are integrated with the management process.



## Control Environment

- Control Environment**
- Sets tone of organization-influencing control consciousness of its people.
  - Factors include integrity, ethical values, competence, authority, responsibility.
  - Foundation for all other components of control.





## Understanding the Control Environment

- How centralized or decentralized is the organization?
- The organization's:
  - Risks
  - Key Processes
  - Control objectives
  - Control activities
- Within the control environment there should be controls in place:
  - Hiring practices
  - Training programs
  - Whistleblower policies
  - Code of Ethics
  - Governance / Oversight Structure

7



## Evaluate Internal Controls at the Entity and Process Levels

- **Entity level** – Your organization as a whole.
  - Generally accomplished through observation, inquiry & inspection.
  - An "Internal Control Management Evaluation Tool" is designed to help organizations perform a systematic, organized, and structured approach to assessing the internal control structure. It is an industry best practice.
- **Process level** - Major functions within an assessable unit or significant account.
  - Evaluating internal control at the process (transaction) level is generally accomplished through detailed testing.

8



## Key Process Documentation

- Determine the extent of available documentation.
- Leverage existing documentation.
- Document process documentation/controls in case no documentation exists.
- Update documentation for changes in **operations**.
- Types of documentation that can be used include:
  - Process Narratives
  - Organizational charts
  - Flowcharts
  - Questionnaires
  - Cycle memorandums
  - Checklists

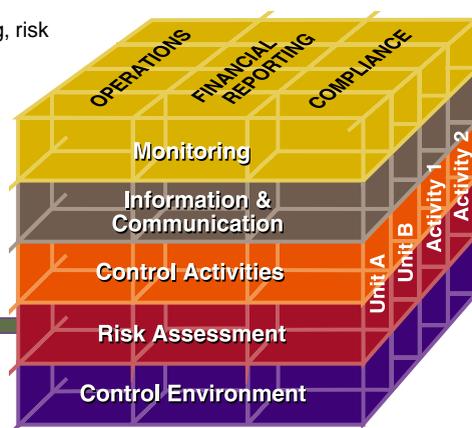
9



## Risk Assessment

Because risks are constantly changing, risk assessment is an ongoing process.

- Risk Assessment**
- Risk assessment is the identification and analysis of relevant risks to achieving the entity's objectives-forming the basis for determining control activities.



10



## Risk Management vs. Risk Assessment

### Risk Management:

A **process** applied in a strategic setting and across the entity, designed to identify and manage risks to stay within risk appetite/tolerance level, to provide reasonable assurance about achieving entity goals and objectives.

### Risk Assessment:

An **element of internal control** within the risk management process that enables management to identify key controls, what actions are required to meet the key control objectives, and what negative consequences may ensue by not accomplishing the key control objectives.

11



## Risk Areas

### FOUR RISK AREAS

#### 1. Strategic

Political risk, talent and succession planning, dependencies on other organizations, etc.

#### 2. Financial

Reporting integrity, audit findings, adjustments, etc.

#### 3. Compliance

Fraud, fair employment practices, etc.

#### 4. Operational

Programs fail to meet objectives, natural disasters, technology availability, functions performed by third parties, etc.

12



## Risk Assessment – Developing a Risk Universe

### SURVEYING THE ENVIRONMENT

1. Knowledge of Strategic Initiatives
2. Insight into Funding Priorities
3. Programs/Activities Exposure to Scrutiny
4. Existing Findings and Recommendations
5. Internal Control Assessments (Internal/External)
6. IT Security Weaknesses

13



## Risk Identification & Analysis

### Internal considerations

1. Use of various qualitative and quantitative methods
2. Discussion with Senior-Level Managers
3. Employee awareness and upward communication
4. Impact of downsizing on personnel/poor succession planning
5. Employee sabotage and system security weaknesses

### External considerations

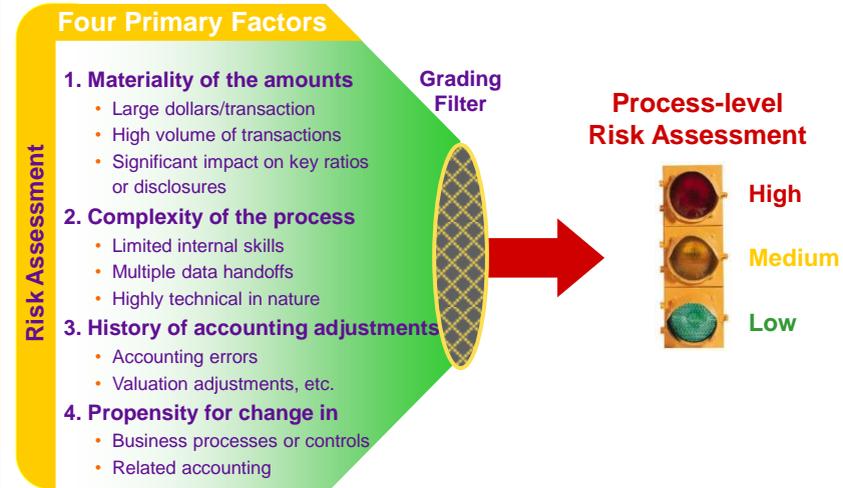
1. Technological advancements
2. Shared services and external audit findings
3. Changing legislative requirements and new laws/regulations
4. Decentralized organization operations
5. Impact of program, political and economic changes

14



## Evaluating Financial Risk

Risk assessment should occur at the business process level as well as the entity level



## Rate Identified Risks

Develop rating criteria that are meaningful to your organization

### Likelihood of risk occurring

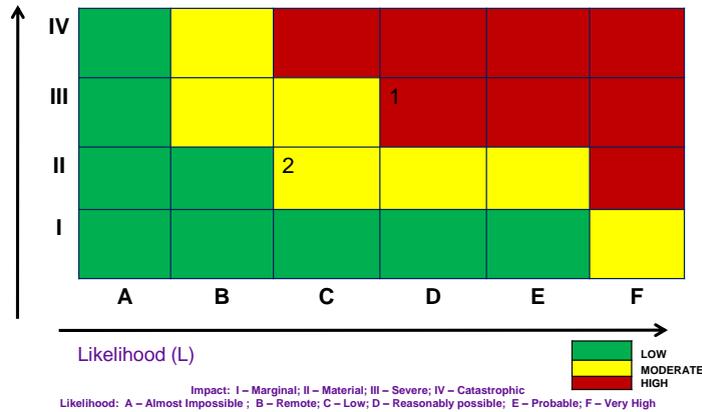
- A – Almost Impossible
- B – Remote
- C – Low
- D – Reasonably Possible
- E – Probable
- F – Very High

### Impact if risk occurs

- I – Marginal
- II – Significant
- III – Severe
- V - Catastrophic



## Risk Mapping



*Consider the organization's risk tolerance and risk appetite related to the risk response*

17



## Risk Strategies

- **Avoidance** - Do not proceed with the activity
- **Mitigation** - Reduce the likelihood/impact through improved control
- **Transfer**- Shift responsibility to an external party
- **Acceptance** - Accept the level of risk
- **Creation** – Seek risk activities strategically in an effort to maximize opportunities

18



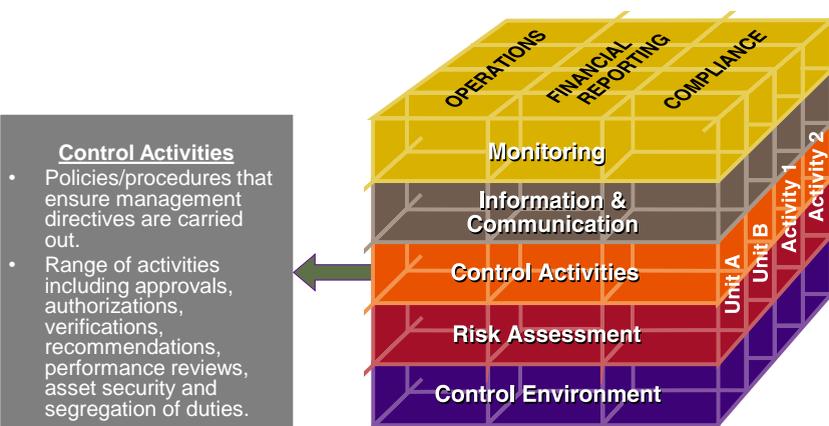
## Risk Management – Key Concepts

1. What are the organization's desired outcomes for stakeholders and beneficiaries?
2. What key processes support those objectives and outcomes?
3. Identify risks associated with those processes
4. Use internal controls to mitigate potential risks
5. Monitor and test internal control effectiveness periodically
6. Report control effectiveness and residual risk to the organization's governance structure

19



## Control Activities



20



## Internal Control Types

Understanding internal control requires knowledge of the types of control and the purpose.

Controls come in two main flavors:

- Preventive vs. detective
- Manual vs. automated

### Examples:

- Segregation of duties
- Access control
- Independent reviews
- Reconciliations
- Approvals

21



## Internal Control - Preventive vs. Detective

- Preventive Control
  - Prevent the occurrence of a negative event in a proactive manner
    - Physical controls (safeguarding of assets)
    - Segregation of duties
    - Application security
    - Application software embedded checks and validations
- Detective Control
  - Detect the occurrence of a negative event after the fact in a reactive manner
    - Direct function reviews
    - Top-level reviews (secondary or compensating)
    - Performance indicators
    - Audits/Program Reviews

22



## Internal Control - Automated vs. Manual

- Automated Control
  - Built into network infrastructure and software applications, for example
    - Passwords
    - Data entry validation checks
    - Batch controls
- Manual Control
  - Require action to be taken by employees, for example
    - Obtaining supervisor's authorization for overtime worked
    - Reconciling bank accounts
    - Matching delivery notes to purchase orders

23



## Identify Key Controls

- Identify and document all controls associated with key processes
- Identify the characteristics of controls that, when functioning as intended, would provide the evaluator with a "level of comfort" to conclude that the control is effective with respect to a given risk.
- Consider control effectiveness by focusing on:
  - Directness and clarity of the control technique
  - Frequency with which the control technique is applied
  - Experience of personnel performing the control
  - Procedures followed when a control identifies an exception condition

24



## Understand Control Design – Financial Controls

Once the key controls are identified, document the controls' design. When documenting, consider:

1. If the controls mitigate risk to an acceptable level.
2. How do potential misstatements affect the related financial report line item?
3. How do the related control objectives prevent or detect the potential misstatement?
4. Are identified control techniques likely to help achieve the control objectives?

25



## Risks of Weak Internal Controls

- Financial misstatements
- Business loss
- Loss of funds or materials
- Lack of management oversight
- Incorrect or untimely management information
- Fraud or collusion
- Tarnished reputation with the public
- Program Sustainability

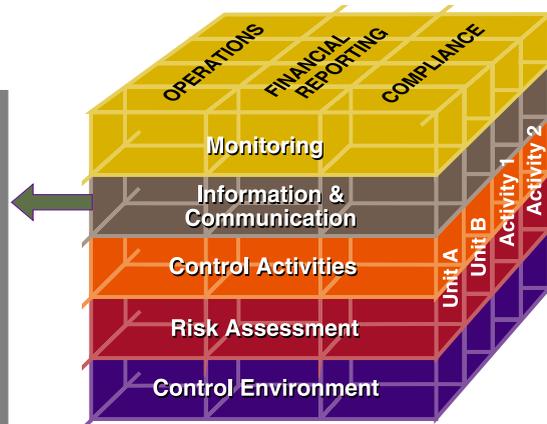
26

## Information & Communication



### Information and Communication

- Pertinent information identified, captured and communicated in a timely manner.
- Access to internally and externally generated information.
- Flow of information that allows for successful control actions from instructions on responsibilities to summary of findings for management action.



27

## Information & Communication Basics



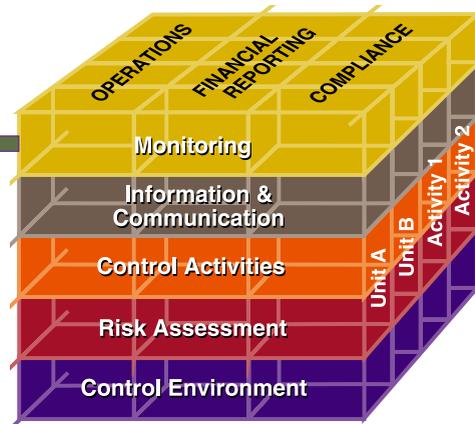
- Effective communication about initiatives within the organization to employees supports successful implementation of internal control activities.
- Likewise, communication with external stakeholders can directly affect the achievement of the organization's objectives and goals.
- Information and Communication allows for the timely exchange of internal and external information across all organizational levels.
- It enables employees to meet their internal control responsibilities and allows for the methods and records established to record, process, summarize, and report transactions and to maintain accountability.

28



## Monitoring

- Monitoring**
- Assessment of a control system's performance over time.
  - Combination of ongoing and separate evaluation.
  - Management and supervisory activities.
  - Internal audit activities.



29



## Monitoring Basics

- Monitoring assesses the performance of an internal control system over a period of time.
- It confirms that the findings of audits and other reviews are promptly resolved so that internal controls are not compromised.
- Helps validate the internal control system is operating as expected.
- Monitoring should be directed at both internal and external risks to the organization.
- Monitoring also consists of supervisory review and sign off to help ensure proper checks and balances.
- Your organization should have a strategy for effective ongoing monitoring.

30



## Test Control Process

- **Identify** transactions to be tested and the key controls.
- **Ascertain** the applicable standards to the transactions (i.e., criteria to judge compliance effectiveness)
- **Select** the appropriate type of testing.
- **Determine** extent of testing.
- **Create** test plan.
- **Conduct** tests for effectiveness.
- **Document** testing and results.
- **Assess** test results.
- **Communicate** findings and recommendations

31



## Planning the Testing Process – Financial Controls

- List of key controls intended to be tested and the method(s) to be used for actual testing.
- Designed to test an adequate number of key controls to ensure an entity can make all relevant financial assertions related to significant accounts.
- Risk-based testing includes identification of key processes and controls and developing test procedures and sampling that is appropriate for the related risk to the organization.

32



## Validate Control Design

- **Deficiency in Design** – A deficiency in design exists when a control that is critical to meet the control objective is not properly designed so that even if the control operates as designed, the control objective is not always met.
  - There are various factors to consider when validating the control design (how control is performed, who performs the control, what data/reports used in performing control, what physical evidence is produced from the control).
  - To determine design effectiveness, work off of the process narratives, flowcharts and any other relevant material that were obtained and/or completed in the documentation stage.
  - Be aware application controls are either programmed control procedures (e.g., edits, matching, reconciliation routines) or computer processes (e.g., calculations, on-line entries, automatic system interfaces).

33



## Confirm Control Effectiveness

- **Deficiency in Operation** – A deficiency in operation exists when a properly designed control does not operate as intended, or when the person performing the control does not possess the necessary authority or qualification to perform the control effectively.
  - Testing operating effectiveness includes, in part:
    - Reviewing supporting documentation for proper authorization,
    - Reviewing the results of periodic reconciliations, and
    - Reviewing policies and procedures to determine if they are being followed.
  - Use appropriate sampling techniques as necessary.

34



## Document Test Results

- Documentation should be maintained for the following:
  - The evaluation of internal control at the entity and process level, and testing of controls,
  - Identified deficiencies.
- Documentation must contain sufficient information to:
  - Enable a knowledgeable person with no previous connection to the assessment to understand the nature, timing, extent, and results of the procedures performed,
  - Understand the evidence obtained,
  - Support the conclusions reached,
  - Determine who performed the work and the date the work was completed.

35



## Conclude



- The results of testing internal controls will support management's judgment as to the effectiveness of controls.

36



## Report – Financial Control Exceptions

The results of testing internal controls should be reported internally and externally as required.

Term	Definitions
<b>Material weakness</b>	A deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.
<b>Significant Deficiency</b>	A deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

37



## Assessing Your Learning Objectives

Questions??

## Grant Thornton Presenters



Name	Title	Telephone	E-mail
Bob Childree	Director	210-881-1770	Bob.Childree@us.gt.com
John Short	Partner	703-637-2960	John.Short@us.gt.com
Ben Kohnle	Partner	214-561-2260	Ben.Kohnle@us.gt.com
Greg Wallig	Managing Director	703-847-7611	Greg.Wallig@us.gt.com
John McLain	Principal	703-837-4460	John.McLain@us.gt.com