Agenda

- Introduction
- Components Overview
- Impact on IT
- Gap Analysis Trends
COSO Introduction
Introduction to COSO 2013


- Companion documents:
  - Internal Control – Integrated Framework: Executive Summary
  - Illustrative Tools for Assessing Effectiveness of a System of Internal Control
  - Internal Control over External Financial Reporting: A Compendium of Approaches and Examples

COSO 1992 Framework will be available until December 15, 2014, then superseded.
Driving the change

Since the inception of the original Framework:

1. Business has changed dramatically –
   - Increasingly global
   - More complex
   - Driven by technology

2. Investors are more engaged –
   - Seeking greater transparency
   - Demand greater accountability for the integrity of internal control systems that support organizations’ operations, governance and external communications

3. Regulatory Regimes have expanded –
   - Additional forms of external reporting are emerging

The COSO Board decided to update the original Framework to make it more relevant to investors and other stakeholders.
**COSO 2013 Framework – Summary of Changes**

**What is *not* changing...**

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Each of the five components of internal control are required for effective internal control
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

**What is changing...**

- Updated for changes in business and operating environments
- Expanded operations and reporting objectives suitable for other purposes
- Implicit fundamental concepts underlying five components codified as 17 principles
- Updated for increased relevance and dependence on IT
- Addresses fraud risk assessment and response (Principle #8)
Components and principles

Under the 2013 COSO Framework, effective internal control requires the following:

- Each of the 5 components and 17 principles must be present and functioning.
- The 5 components must operate together in an integrated manner.
- All 81 points of focus are considered, but are not required to be present.
Applying the framework – key concepts

Each of the **five components and relevant principles** is present and functioning.

- **“Present”** refers to the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives.

- **“Functioning”** refers to the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objective.

The five components operate together in an integrated manner.

- **“Operating together”** refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective. Components should not be considered discretely; instead, they operate together as an integrated system.
Interaction among COSO Components

Controls related to the COSO components can be found at the entity level and transaction level.

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Risk Assessment</th>
<th>Information and Communication</th>
<th>Monitoring Activities</th>
<th>Control Activities</th>
</tr>
</thead>
</table>

**Entity-Level Controls (ELCs)**

**Higher-Level Controls (HLCs)**

**Process-Level Controls (PLCs)**

**GITCs**

- Controls that do not specifically relate to an assertion (indirect)
- Controls that specifically relate to an assertion (direct)
Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The resulting control environment has a pervasive impact on the overall system of internal control.

**Control Environment – 2013 Framework Changes**

- Captures seven (7) factors in 1992 Framework into five (5) principles
- Explains that Control Environment is the foundation for a sound system of internal control
- Addresses changes in business models – the globalization of the business and its operations
- Expands and clarifies guidance on:
  - Governance roles in an organization, recognizing differences in structures, types of entities, etc.
  - The need to consider internal control across the expanded organization, including outsourced service providers and other external partners
  - Expectations of competence and accountability with respect to internal control
1. The organization demonstrates a commitment to integrity and ethical values.

Points of Focus

• **Sets the *Tone at the Top***
  - Board of Directors and management at all levels demonstrate through directives, actions and behavior the importance of integrity and ethical values to support functioning system of internal control

• **Establishes Standards of Conduct**
  - The expectation of the Board of Directors and senior management concerning integrity and ethical values are defined in Standards of Conduct and understood throughout the organization and by outsourced service providers and business partners

• **Evaluates adherence to Standards of Conduct**
  - Processes are in place to evaluate the performance of individuals and teams against the Standards of Conduct

• **Addresses deviations in a timely manner**
  - Deviations in Standards of Conduct are identified and remedied in a timely consistent manner
Tone at the top and throughout the organization is fundamental to the functioning of an internal control system.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Points of Focus

• Establishes oversight responsibilities
  – The Board of Directors (BoD) identifies and accepts its oversight responsibilities in relation to the established requirements and expectations

• Applies relevant expertise
  – The BoD defines, maintains and periodically evaluate the skills and expertise needed to enable them to ask probing questions of senior management and take commensurate actions

• Operates independently
  – The BoD has sufficient independent members and is objective in evaluations and decision making

• Provides oversight for the system of internal control
  – The BoD retains oversight responsibilities for management’s design, implementation and conduct of internal control
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

### Points of Focus

- **Considers all structures of the entity**
  - Management and the BoD considers multiple structures (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.

- **Establishes reporting lines**
  - Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and the flow of information to manage the activities of the entity.

- **Defines, assigns, and limits authorities and responsibilities**
  - Management and the BoD delegate authority, define responsibilities and use appropriate processes and technology to assign responsibility and segregate duties at various levels of the organization (e.g., the Board; senior executives; management; personnel; outsourced service providers).
Principle # 4: Competence and Effective Controls

<table>
<thead>
<tr>
<th>Needs Assessment</th>
<th>Principle # 4</th>
<th>Effective Control Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior managers’ competence requirements per Board of Directors</td>
<td>Subject matter experts</td>
<td>At all levels</td>
</tr>
<tr>
<td>Job descriptions for employees</td>
<td>Relevant experience</td>
<td>At third party service providers</td>
</tr>
<tr>
<td></td>
<td>Proper succession planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GAAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEC rules &amp; regulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tax laws</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Others laws &amp; regulations</td>
<td></td>
</tr>
</tbody>
</table>

Demands for greater competence and accountability increase as organizations grow more complex, acquire entities, restructure, introduce new products and services, and implement new processes and technologies.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Points of Focus

- **Establishes policies and practices**
  - Polices and practices reflect expectations of competence necessary to support the objectives

- **Evaluates competence and addresses shortcomings**
  - The Board of Directors and management evaluate competence across the organization and at outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings

- **Attracts, develops, and retains individuals**
  - The organization mentors and trains to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives

- **Plans and prepares for succession**
  - Senior management and the Board of Directors develop contingency plans for assignment of responsibility important for internal control
Control Environment: Principle #5 and Points of Focus

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Points of Focus

- **Enforces accountability through structures, authorities, and responsibilities**
  - Establishes the mechanisms to communicate and holds individuals accountable for internal control responsibilities across the organization and implement corrective action

- **Establishes performance measures, incentives, and rewards**
  - . . . . appropriate for responsibilities at all levels of the entity, reflecting performance and Standards of Conduct, considering achievement of ST and LT objectives

- **Evaluates performance measures, incentives, and rewards for ongoing performance**
  - Aligns incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives

- **Considers excessive pressures**
  - Evaluates and adjusts pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures and evaluate performance

- **Evaluates performance and rewards or disciplines individuals**
  - Evaluates performance of internal control responsibilities, including adherence to Standard of Conduct and expected competence; provides rewards or disciplinary action as appropriate
Control Environment: Key Learning Points

- Scoping of ICOFR across the organization and at all levels
- Internal control at third-party service providers and other outside partners
- Increased oversight responsibilities of the board of directors
- Importance of clearly defined lines of reporting and authority
- Competence and accountability – key to effective control activities/ICOFR
- Performance measurement and incentive programs that encourage effective execution of ICOFR responsibilities
Risk Assessment

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Thus, risk assessment forms the basis for determining how risks will be managed.

Risk Assessment – 2013 Framework Changes

- Recognizes that many organizations take a risk-based approach to internal control
- Clarifies that risk assessment includes processes for risk identification, risk analysis, and risk response
- Expands the discussion on:
  - Risk tolerances (acceptable risk levels) and responses to identified risks
  - Assessment of significance of risks
  - The need to understand significant changes in internal and external factors and the impact of these changes on the system of internal control
- Includes specific assessment of fraud risk
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Points of Focus

- **External Financial Reporting Objectives**
  - Separately set out characteristics related to operations; external financial reporting; external non-financial reporting; internal reporting; compliance objectives

- **Complies with applicable accounting standards**
  - Financial reporting objectives are consistent with accounting principles suitable and available for the entity
  - Accounting principles selected are appropriate in the circumstances

- **Considers Materiality**
  - Management considers materiality in financial statement presentation

- **Reflects entity activities**
  - External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions
Risk Assessment: Principle #7 and Points of Focus

7. 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.

Points of Focus

• Includes entity, subsidiary, division, operating unit, and functional levels
  – The organization identifies and assesses risks at the entity, subsidiary, division, operating unit and functional levels relevant to the achievement of objectives

• Analyzes internal and external factors
  – Risk identification considers both internal and external factors and their impact on the achievement of objectives

• Involves appropriate levels of management
  – The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management

• Estimates significance of risks identified
  – Identified risks are analyzed through a process that includes estimating the potential significance of the risk

• Determines how to respond to risks
  – Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce or share the risk
Principle # 7: Ongoing Iterative Process

- New product or service lines
- Geographical expansion
- New executive leadership
- Turnover in key financial reporting positions
- New environmental laws
- New stock exchange regulations
- Business combinations
- Restructuring

Identify and assess risks at the entity, subsidiary, division, operating unit and functional levels.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of Focus

- **Considers various types of fraud**
  - The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption [and management override of controls] resulting from the various ways that fraud and misconduct can occur

- **Assesses incentives and pressures**
  - The assessment of fraud risk considers incentives and pressures

- **Assesses opportunities**
  - The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity’s reporting records, or committing other inappropriate acts

- **Assesses attitudes and rationalizations**
  - The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions
Risk Assessment: Key Learning Points

- Risk assessment is an ongoing and iterative process
- Materiality and risk tolerances need to be defined by management
- Risk assessment should be updated on an at least annual basis
- Fraud risks need to be considered in the risk assessment process
- Risk assessment should be performed at entity level and cascaded throughout the organization
- Early warning controls should identify impact of changes in internal and external factors
Control Activities

Control activities are the actions established through policies and procedures to mitigate risks to the achievement of objectives. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment.

**Control Activities – 2013 Framework changes**

- Updated for the evolution in technology since 1992
- Addresses the linkage between business processes, automated control activities and GITCs
- Contrasts process-level controls from controls at other levels of the organization
- Updates GITC applicability across all technology platforms
- Clarifies that control activities are actions established by policies and procedures rather than being the policies and procedures themselves
Control Activities: Principle #10 and Points of Focus

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Points of Focus

• Integrates with Risk Assessment
  − Control activities help ensure that the risk responses that address and mitigate risks are carried out

• Considers entity-specific factors
  − Management considers how the environment, complexity, nature and scope of its operations affect the selection and development of control activities

• Determines relevant business processes
  − Management determines which relevant business processes require controls activities

• Evaluates a mix of control types
  − Control activities include a range and variety of controls; considering both manual and automated controls, and preventative and detective controls

• Considers at what level controls are applied
  − Management considers control activities at various levels of the organization

• Addresses segregation of duties
  − Management segregates incompatible duties and where not practical, selects and develops alternative control activities
Principle # 10: Implementing Control Activities Responsive to Risks

Understand the process – how transactions are initiated, authorized, processed and recorded

Identify financial reporting risks – the What Could Go Wrongs (WCGWs)

- Controls should be responsive to the risks to control objectives
- Confusion over nonroutine, complex transactions when the control becomes the process
- Flowcharting to describe the business processes or transaction flows and identify points where a risk of error could occur

Every time the data moves, we are likely to have a WCGW related to the CEA of data
### Control Activities: Principle #11 and Points of Focus

#### 11. The organization selects and develops general control activities over technology to support the achievement of objectives.

**Points of Focus**

- **Determines dependency between the use of technology in business processes and GITCs**
  - Management understands and determines dependency and linkage between business processes, automated controls activities and GITCs

- **Establishes relevant Technology Infrastructure control activities**
  - Which are designed and implemented to help the completeness, accuracy and availability of technology processing

- **Establishes relevant Security Management Process control activities**
  - Which are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity’s assets from external threats

- **Establishes relevant Technology Acquisition, Development, and Maintenance Process control activities**
  - Management selects and develops control activities over the acquisition, development and maintenance of technology and its infrastructure to achieve objectives
Principle # 11: Dependency and Linkage Among Processes and Controls

Financial Statements

Purchasing
- Automated Activity
- Automated Activity

A/P
- Automated Activity

Operating Expenses
- Automated Activity

Master File

Applications
Databases
Operating Systems
Control Activities: Principle #12 and Points of Focus

12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Points of Focus

- Establishes policies and procedures to support deployment of management’s directives
  - Controls are built into business processes through specific policies and procedures
- Establishes responsibility and accountability for executing policies and procedures
  - Management assigns responsibility and accountability for the controls in the business unit or function where the risk resides
- Performs in a timely manner
  - Responsible personnel perform controls in a timely manner
- Takes corrective action
  - Responsible personnel investigate and act on matters identified as a result of executing the control
- Performs using competent personnel
  - Competent personnel with sufficient authority perform controls with diligence and continuing focus
- Reassesses policies and procedures
  - Management periodically reviews controls to determine their continued relevance and refreshes them when necessary
Control Activities: MRC Evidence

Not all MRCs require the same level of judgment or technical expertise, and thus require varying levels of evidence.

<table>
<thead>
<tr>
<th>MRC Type</th>
<th>Examples</th>
<th>Characteristics</th>
<th>Evidence Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control where the degree of judgment is low</td>
<td>• Bank Reconciliation&lt;br&gt;• Recurring Manual Journal Entry Approval (e.g., Payroll Accrual)</td>
<td>• Review is objective in nature&lt;br&gt;• Source data comes from well controlled systems with limited to no manipulation&lt;br&gt;• Limited judgment&lt;br&gt;• Defined level of precision (i.e. thresholds) that is documented and consistently applied</td>
<td>• Sign-off by authorized reviewer&lt;br&gt;• Appropriate supporting documentation&lt;br&gt;• Amounts in supporting documentation tie to journal entries</td>
</tr>
<tr>
<td>Control where the degree of judgment is significant</td>
<td>• Bad Debt Reserve Review&lt;br&gt;• Impairment Review</td>
<td>• Subject to assumptions and estimates&lt;br&gt;• Defined level of precision&lt;br&gt;• Defined level of precision (i.e. thresholds) that is documented and consistently applied</td>
<td></td>
</tr>
<tr>
<td>Higher-level control that monitors the effectiveness of other controls and degree of judgment is moderate</td>
<td>• Variance Analysis (e.g. Budget to Actual)&lt;br&gt;• Financial Statement Review</td>
<td>• Data used in calculations might not come solely from a system</td>
<td>• Sign-off by authorized reviewer&lt;br&gt;• Evidence of review&lt;br&gt;− Notes/tickmarks&lt;br&gt;− Memo or bullets summarizing review&lt;br&gt;• Evidence of exceptions identified&lt;br&gt;− Highlighting&lt;br&gt;− Notes/tickmarks&lt;br&gt;• Evidence of resolution&lt;br&gt;− Emails&lt;br&gt;− Memos/Minutes</td>
</tr>
</tbody>
</table>
When using system generated reports, completeness and accuracy of data should be verified by the reviewer, with evidence retained.

### System Generated Reports

- For reports where parameters (e.g. date ranges) were used to generate the information, how do you know that the correct ranges were used? *This can be evidenced by including a screenshot of the parameters with the control evidence.*
  - *Running a report that is then used in a subsequent calculation or analysis*

- For standard reports that do not require the user to input parameters or generate a query in a non-modifiable format, no further action is necessary by the control owner. Assurance on those systems will be completed as part of ITGC testing. If relevant ITGCs fail during testing, additional procedures will be performed to determine completeness and accuracy.
  - *A/R Aging report exported to a PDF*
  - *Reports from a third-party; assuming their SSAE 16 has an unqualified opinion*
When using spreadsheets, completeness and accuracy of data should be verified by the reviewer, with evidence retained.

### Spreadsheets

- Spreadsheet documentation requirements (this applies to **spreadsheets that are a part of a key control**):
  - Source data should be clearly documented on the spreadsheet
  - Notation on the control evidence on how formulas were verified for accuracy, could include:
    - Re-performance of a sample of formulas AND/OR
    - Review of assumptions and cell references
- Access to be restricted on key spreadsheets, and should be stored on a network and backed up periodically
Key Reminders – Control Activities

- Understand the source and flow of information, identify WCGWs and controls that address them
- Understand how GITCs support application controls
- Consider outliers and level of precision in evaluating MRCs
- Evaluate controls around the completeness and accuracy of information used in MRCs
Information & Communication

Information is necessary for entity to carry out internal control responsibilities to support achievement of objectives. Communication is continual, iterative process of providing, sharing, and obtaining necessary information.

Information & Communication – 2013
Framework Changes

- Emphasizes importance of quality of information.
- Expands discussion on:
  - Impact of regulatory requirements on reliability and protection of information
  - Volume and sources of information in light of increased complexity of business processes, greater interaction with external parties, and technology advances
- Reflects impact of technology and other communication mechanisms on speed, means, and quality of information flow
13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

Points of Focus

- **Identifies information requirements**
  - A process is in place to identify the information required and expected to be support the functioning of the other components and achievement of the entity’s objectives

- **Captures internal and external sources of data**
  - Information systems captures internal and external sources of data

- **Processes relevant data into information**
  - Information systems process and transform relevant data into information

- **Maintains quality throughout processing**
  - Information systems produce information that is timely, current, accurate, complete, accessible, protected and verifiable and retained. Information is reviewed to assess its relevance in supporting the components

- **Considers costs and benefits**
  - The nature, quantity and precision of information communicated is commensurate with and support the achievement of objectives
Principle # 13: Relevant Information to Right Person at Right Time

- **Control Activity**: Review of Tax Provision by Tax Director

  - **New tax laws in Japan**
    - Japanese flag

  - **New related party supplier in India**
    - American flag
    - Indian flag

  - **New business in Canada**
    - Canadian flag

  - **Employees working out-of-state**
    - Oklahoma flag
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.

Points of Focus

- **Communicates internal control information**
  - A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities
- **Communicates with the Board of Directors**
  - Communication exists between management and BoD so that both have information needed to fulfill their roles
- **Provides separate communication lines**
  - Separate communication channels, such as whistle blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication
- **Selects relevant method of communication**
  - The method of communication considers the timing, audience and nature of the information
Information and Communication: Principle #15 and Points of Focus

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Points of Focus

• **Communicates to external parties**
  – Processes are in place to communicate relevant and timely information to shareholders, partners, regulators, customers, financial analysts and other parties

• **Enables inbound communications**
  – Open communication channels allow management and BoD to receive relevant input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others

• **Communicates with the Board of Directors**
  – Relevant information from assessments conducted by external parties is communicated to the BoD

• **Provides separate communication lines**
  – Separate communication channels, such as whistle blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication

• **Selects relevant method of communication**
  – The method of communication considers the timing, audience and nature of the communication and legal, regulatory, and fiduciary requirements and expectations
Principle # 15: External Communications

Reporting Entity

Stock Exchange

Banks/Lenders
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.

Monitoring Activities – 2013

Framework Changes

- Refines the terminology, where the two main categories of monitoring activities are now referred to as “ongoing evaluations” and “separate evaluations”
- Added the need for a baseline understanding in establishing and evaluating ongoing and separate evaluations
- Expanded discussion of the use of technology and external service providers
Monitoring Activities: Principle #16 and Points of Focus

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Points of Focus

- **Considers a mix of ongoing and separate evaluations**
- **Considers rate of change**
  - Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
- **Establishes baseline understanding**
  - The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
- **Uses knowledgeable personnel**
  - Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
- **Integrates with business processes**
  - Ongoing evaluations are built into the business process and adjust to changing conditions.
- **Adjusts scope and frequency**
  - Management varies the scope and frequency of separate evaluations depending on risk.
- **Objectively evaluates**
  - Separate evaluations are performed periodically to provide objective feedback.
Monitoring Activities: Principle #17 and Points of Focus

17. 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.

Points of Focus

- **Assesses results**
  - Management and the BoD assess the results of ongoing and separate evaluations

- **Communicates deficiencies**
  - Deficiencies are communicated to the parties responsible for taking corrective action and to senior management and BoDs, as appropriate

- **Monitors corrective actions**
  - Management tracks whether deficiencies are remediated on a timely basis
Principle # 17: Evaluation of Control Deficiencies

**Six Steps in Evaluating Control Deficiencies**

1. Determine whether a control deficiency exists
2. Identify and describe the control deficiency
3. Determine whether the control deficiency is indicative of other deficiencies
4. Evaluate the severity of the deficiency by considering magnitude and likelihood of the potential misstatement
5. Identify relevant compensating controls and conclude on the severity
6. Aggregate similar deficiencies and evaluate the aggregated deficiencies for severity
“... where management has outsourced certain functions to third-party service providers, management maintains responsibility to assess the controls over the outsourced operations.”

Management should consider the applicability of all 17 COSO Principles for financially significant business processes supported by third-party service providers.
### Distinction Between Monitoring Activities and Control Activities

<table>
<thead>
<tr>
<th><strong>Control Activity</strong></th>
<th><strong>Monitoring Activity</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operates at precision level to address risks for specific financial statement assertions</td>
<td>Does not operate at precision level to address risks for specific financial statement assertions</td>
</tr>
<tr>
<td>Responds to a specified risks (WCGWs)</td>
<td>Monitors effective operation of control activities</td>
</tr>
<tr>
<td>Designed to detect and correct errors in financial statement assertions</td>
<td>Monitors remediation of deficiencies</td>
</tr>
</tbody>
</table>

**Monitoring activities assess whether controls in each of five components are operating as intended**

**Monitoring activities are NOT a substitute for control activities—BOTH are important**
Key Reminders – Monitoring Activities

- Use an appropriate mix of ongoing and separate evaluations
- Identify the root cause of a deficiency
- Determine whether a deficiency is indicative of other deficiencies.
- Determine whether there is a reasonable possibility that the deficiency or group of deficiencies would result in a material misstatement
Impact on Information Technology
Control Environment

### Principles 1 – 5

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

### IT Considerations

- Is IT properly positioned in the organization?
- Are the organizational structures and reporting lines appropriate?
- Are IT-related policies sufficiently designed to enable achievement of business objectives?
- What processes are in place to handle IT policy violations?
- Does the Board have adequate expertise in IT and what type of IT-related issues do they provide oversight on?
- Is there significant turnover in the IT function?
- Do employees have current and appropriate IT skills/knowledge?
- How does the organization measure IT performance?
## Principles 6 – 9

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. 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.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

## IT Considerations

- Have systems/data been considered during risk assessment activities?
- Are IT regulatory requirements, standards, and frameworks considered and/or implemented?
- Is end user and, if applicable, cloud computing considered in the risk assessment?
- Is IT considered in fraud risk assessments, including threats from internal and external sources?
- Is the impact of IT change (e.g. implementations, upgrades, etc.) considered by all levels of management?
## Control Activities

<table>
<thead>
<tr>
<th><strong>Principles 10 – 12</strong></th>
<th><strong>IT Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10.</strong> The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</td>
<td>Has the organization documented business process reliance on technology?</td>
</tr>
<tr>
<td><strong>11.</strong> The organization selects and develops general control activities over technology to support the achievement of objectives.</td>
<td>Is technology used to automate control activities?</td>
</tr>
<tr>
<td><strong>12.</strong> The organization deploys control activities through policies that establish what is expected and procedures that put policies into place.</td>
<td>Are application controls sufficiently designed and tested to confirm completeness, accuracy, and validity assertions?</td>
</tr>
<tr>
<td></td>
<td>Can applications be used to enforce segregation of duties?</td>
</tr>
<tr>
<td></td>
<td>Are applications designed to have a mix of preventative and detective activities?</td>
</tr>
<tr>
<td></td>
<td>Have system configurations been effectively designed and reviewed?</td>
</tr>
</tbody>
</table>
Principles 13 – 15

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

IT Considerations

- Is information provided by third parties reliable?
- Are sufficient information governance activities established?
- How is data integrity and quality assured and can it be relied on to make critical business decisions?
- How can data be used to enhance internal control and reduce fraud risk?
- How is customer or other confidential data protected?
- Are processes and systems in place to ensure regulatory agencies receive accurate and complete data in a timely manner?
Monitoring

**Principles 16 – 17**

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. 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.

**IT Considerations**

Are technology activities captured in audit histories and properly monitored?

Are incidents responded to and resolved?

Is the organization competent enough in IT such that they can evaluate technology risk?

Does the organization perform technology risk assessments to identify and address targets of opportunity?

Does the organization use data analysis to proactively manage potential risks?
Gap Analysis Trends
COSO 2013 Gap Analysis engagements have yielded similar observations:

- Several controls can be required to address a point of focus or principle.
- Gaps in direct entity level controls and process level controls have been indicators of weak or deficient indirect entity level controls.
- When an applicable principle is not present and functioning, the associated component has been determined to not be present and functioning.
- Gaps can be classified as:
  - Principle Gaps: Sufficient controls do not exist to achieve the COSO Principle.
  - Attribute Gaps: Though controls exist, an important attribute is missing.
  - Evidence Gaps: Insufficient evidence exists to confirm the control operated as designed.
  - Testing Gaps: Though a control may have operated, sufficient testing was not performed.
## Gap Definitions and Examples

<table>
<thead>
<tr>
<th>Gap Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle Gap</td>
<td>Sufficient controls do not exist to achieve the COSO Principle</td>
<td>A Company’s Finance Department performs a financial risk assessment; however, an IT risk assessment is not performed which assesses the risk of use, acquisition, modification, and operation of IT within an enterprise. The absence of an IT risk assessment is a missing process and control.</td>
</tr>
<tr>
<td>Attribute Gap</td>
<td>Though controls exist, an important attribute is missing</td>
<td>A Company provides the Information Security Policy to Outside Service Providers (OSPs) and requires acknowledgement; however, the Policy is only written in English and greater than 50% of the OSPs are foreign entities. The absence of the Policy being provided to OSPs in multiple languages is a missing attribute.</td>
</tr>
<tr>
<td>Evidence Gap</td>
<td>Insufficient evidence exists to confirm the control operated as designed</td>
<td>A Company’s IT Steering Committee conducts a review of new projects; however, meeting minutes lack evidence to support the assessment of an ERP implementation. Lack of evidence to support the review and approval of an ERP implementation initiative is a control evidence gap.</td>
</tr>
<tr>
<td>Testing Gap</td>
<td>Though a control may have operated, sufficient testing was not performed</td>
<td>A Company’s IT Department conducts an annual review of Service Organization Controls reports; however, the test plan does not address whether management’s review was sufficient to address user control considerations and internal control deficiencies identified in the report. The lack of a test of the sufficiency of review is a testing gap.</td>
</tr>
</tbody>
</table>
Common IT Gaps

We have noted a trend in the following IT gaps:

- Responses to the review of SOC Type I/II reports are not formalized
- Management does not consider IT applications supporting in-scope business cycles during the risk assessment process
- IT process narratives, policies, and system data flow charts are not current
- Management’s testing documentation for GITC’s is incomplete – commonly for end-user computing and security monitoring controls
- Privileged user access management controls (e.g. system administrator rights) are not properly designed, documented, and tested
- Control owners are not consistently defined in control descriptions to establish accountability
- Processes are not in place to validate the completeness and accuracy of data used to support the performance of control activities
- Deficiency logs do not contain management action plans which define what the plans are, who is responsible for remediation, the timeline of when action is required, and the status of remediation
Top 10 Transition Areas

1. Application of the principles and points of focus across the organization and at all levels
2. Evaluation of third party service organization arrangements
3. Board of Director oversight of internal control over financial reporting (Principle #2)
4. How incentives and rewards are aligned with fulfillment of internal control responsibilities (Principle #5)
5. Formal documentation of materiality assessments and risk tolerance (Principles #6 and #10)
6. Fraud Risk Assessment and determination of fraud risk controls (Principle #8)
7. The process for ensuring risk assessment and internal controls are responsive to change (Principle #9)
8. Linking general IT controls to related application controls (Principles #10 and #11)
9. Demonstrating that monitoring activities are built into business processes (Principles #12 and #17)
10. Demonstrating that the 17 principles and five components are present and functioning and that the components work in an integrated manner

And the documentation of controls . . . .
What Questions Do You Have?
©2015 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International Cooperative ("KPMG International").

Sonny Crandall
480-459-3507
scrandall@kpmg.com

Ted Quigley
480-459-3541
tquigley@kpmg.com

Amanthi Pendegraft
480-459-3470
apendegraft@kpmg.com