So What Is COSO? And Why Is it a Big Deal??

CACUBO
May 16, 2016
Lealan Miller, CPA, CGFM
These seminar materials are intended to provide the seminar participants with guidance in accounting and financial reporting matters. The materials do not constitute, and should not be treated as professional advice regarding the use of any particular accounting or financial reporting technique. Every effort has been made to assure the accuracy of these materials. The presenters do not assume responsibility for any individual's reliance upon the written or oral information provided during the seminar. Seminar participants should independently verify all statements made before applying them to a particular fact situation, and should independently determine consequences of any particular technique before recommending the technique to a client or implementing it on the client's behalf.
The “Fraud Triangle”
The "Fraud Triangle"

Motive
The “Fraud Triangle”

Motive

Rationalization
The “Fraud Triangle”

Motive

Perceived Opportunity

Rationalization
• You will not prevent all losses.
• You are trying to prevent large losses
Few things are more devastating, demoralizing, and tragic than the discovery that someone you trusted has committed fraud.

There is, however, one thing that is considerably more devastating, demoralizing, and tragic...

When a totally innocent and honest employee falls under suspicion simply because the lack of internal control created the appearance of an opportunity to commit fraud.
What is the COSO?

• Committee of Sponsoring Organizations of the Treadway Commission (COSO)
• Five Sponsoring Organizations
How Broad are Internal Controls?

- **Institute of Internal Auditors Definition:**
  - A process, effected by an entity's board of directors (governing board), management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

- Includes
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with laws and regulations
Common Themes in COSO since 1992

- **Continuous** improvement on internal control testing and reporting
- **Continuous** understanding of new risks in the environment with regard to audit, technology and management
- **Continuous** process improvement with regard to changes in organizational structure (Google didn’t exist 10 years ago)
- **Continuous** process improvement to detect fraud
  - Each economic cycle brings new challenges to detect / deter fraud

- Consists of three volumes:
  - Executive Summary
  - Framework and Appendices
  - Illustrative Tools for Assessing Effectiveness of a System of Internal Control

- Sets out:
  - Definition of internal control
  - Categories of objectives
  - Components and principles of internal control
  - Requirements for effectiveness
Part #2 – Internal Control over External Financial Reporting: A Compendium of Approaches and Examples

- Illustrates approaches and examples of how principles are applied in preparing financial statements
- Considers changes in business and operating environments during past two decades
- Provides examples from a variety of entities – public, private, not-for-profit, even government
- Aligns with the updated Framework
Internal Control–Integrated Framework

AKA – the Rubik’s Cube of COSO
Update Considers Changes in Business and Operating Environments

Environment changes... have driven Framework updates

- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexity in business
- Demands and complexities in laws, rules, regulations, and standards
- Expectations for competencies and accountabilities
- Use of, and reliance on, evolving technology
- Expectations relating to preventing and detecting fraud
<table>
<thead>
<tr>
<th>Components</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrates commitment to integrity and ethical values</td>
</tr>
<tr>
<td></td>
<td>2. Exercises oversight responsibility</td>
</tr>
<tr>
<td></td>
<td>3. Establishes structure, authority and responsibility</td>
</tr>
<tr>
<td></td>
<td>4. Demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5. Enforces accountability</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>6. Specifies suitable objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identifies and analyzes risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses fraud risk</td>
</tr>
<tr>
<td></td>
<td>9. Identifies and analyzes significant change</td>
</tr>
<tr>
<td>Control Activities</td>
<td>10. Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops general controls over technology</td>
</tr>
<tr>
<td></td>
<td>12. Deploys through policies and procedures</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>13. Uses relevant information</td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
<tr>
<td></td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>
Examples of Each Principle
Components and Principles of Effective Internal Control

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.

Points of Focus:
- Sets the Tone at the Top
- Establishes Standards of Conduct
- Evaluates Adherence to Standards of Conduct
- Addresses Deviations in a Timely Manner

- Points of focus may not be suitable or relevant, and others may be identified
- Points of focus may facilitate designing, implementing, and conducting internal control
- There is no requirement to separately assess whether points of focus are in place
1. A Housing Agency demonstrates a commitment to integrity and ethical values

- **Component:** Control Environment

- **Principle:** Information
  - Technology staff tests for data breaches of personally identifiable information continuously

- **Principle:** Information & Communication
  - Management obtains and reviews data and information underlying potential deviations captured in reports generated immediately upon occurrence

- **Principle:** Monitoring Activities
  - Risk manager separately evaluates Control Environment, considering employee behaviors and whistleblower hotline results and reports thereon
• The Organization has created, maintains, and distributes a code of conduct and ethical standards
• Distributed to all employees and external parties acting on behalf of the Organization, and has posted it on the Organization website.
• Code of conduct is available in all relevant languages for ease of access and understanding by Citizens.
• Organization requires all employees to complete periodic interactive web-based training sessions on various aspects of the code and ethical standards.
• The Organization provides a supplier code of conduct to its vendors as part of its contracting process, which provide a basis for evaluation alongside product / service delivery evaluation.

How is this effective?
Control Objective 1
Control Environment
How Does Your Organization:

1. Demonstrate commitment to integrity and ethical values
2. Exercise oversight responsibility
3. Establish structure, authority and responsibility
4. Demonstrate commitment to competence
5. Enforce accountability
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.
How Various Controls Effect Principles, e.g.,

Risk Assessment

The Controller identifies risks to the achievement of the objectives across the office and analyzes risks as a basis for determining how the risks should be managed.

- As part of the meetings with senior staff on goals and objectives, risks are noted and potential controls against those risks are brainstormed and initiated if approved by the audit committee. **Risk Assessment**
- The result of the brainstorming is communicated to staff as part of semi-annual reviews. **Information & Communication**
- A dashboard of risks is established and is updated with each batch cycle. **Monitoring Activities**
How did we assess risk here and how is it mitigated?
Control Objective 2
Risk Assessment
How Does Your Organization:

6. Specify suitable objectives
7. Identify and analyze risk
8. Assess fraud risk
9. Identify and analyze significant change
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

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

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into place.
The Controller selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Every two years, the Controller rotates duties among the divisional managers not only to provide them with a broader experience but also to lower the risk of financial reporting fraud. Staff enjoys the rotation as they are not working the same job repeatedly.

A report is developed predicting payables over the next 30 days and disseminated to fiscal officers. The payables are compared to encumbrances.

The Comptroller reviews payables that are unusual, or above $5,000 or infrequent.

Control Activity

Information & Communication

Monitoring Activities
An CFO recently evaluated the use of spreadsheets in its financial close process. In doing so, it identified that the spreadsheets supporting the calculation of the fair values of investments, those supporting capital assets, and debt were of high risk, based on their susceptibility to error and significance to the financial statements. The CFO also classified the spreadsheets as high in complexity because they included the use of macros and multiple supporting spreadsheets to which cells and values were interlinked. The spreadsheets were used either as the basis for journal entries into the general ledger or as financial statement disclosures.

How would you solve this?
Control Objective 3
Control Activities
How Does Your Organization:

10. Select and develop control activities
11. Select and develop general controls over technology
12. Deploy through policies and procedures
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.
### How Various Controls Effect Principles, e.g., Information & Communication

<table>
<thead>
<tr>
<th>Component</th>
<th>Control Activity</th>
<th>Monitoring Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle</td>
<td>The operator of a gas station obtains or generates and uses relevant, quality information to support the functioning of internal control.</td>
<td></td>
</tr>
</tbody>
</table>

- **With each credit card transaction**, if the transaction is unauthorized, an error is generated and the attendant is notified. Gas pumps do not work unless cash is paid. *Control Activity*
- **Instances of fraudulent credit cards** are notified immediately to local police via a push button or tie in *Information & Communication*.
- **Video surveillance** is used on all transactions and is monitored by the station owner. Tapes are stored for a minimum of 60 days and are time-stamped. *Monitoring Activities*
The CFO receives a daily update at 8 AM on her desk compiled by staff. The update consists of newspaper clips, other publications, event press releases, and other information from external parties (including social media) to gather information relevant to performing her responsibilities.

Do you have an issue with this?
Components and Principles of Effective Internal Control

Monitoring Activities

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 those charged with governance, as appropriate.
Control Objective 4
Information and Communication

How Does Your Organization:

13. Use relevant information
14. Communicate internally
15. Communicate externally
How Various Controls Effect Principles, e.g.,

<table>
<thead>
<tr>
<th>Component</th>
<th>Principle</th>
<th>Controls embedded in other components may effect this principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Activities</td>
<td>The Controller selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The quality assurance division reports are also transmitted to the division where the problem occurred. Corrective action is taken. If no corrective action is accomplished, the employee’s personnel file contains the issue and if repeated, could be grounds for termination. <strong>Control Activity</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statistical reports on uses of personally identifiable activity are reported to employees on a monthly basis. All employees are trained semi-annually on when/how/who can access PII <strong>Information &amp; Communication</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reports on detections of improper use of personally identifiable information by employees are escalated to a senior review board that investigates all activities and reacts to breaks in accordance with state law. <strong>Monitoring Activities</strong></td>
<td></td>
</tr>
</tbody>
</table>
Control Objective 5
Monitoring
How Does Your Organization:

16. Conduct ongoing and/or separate evaluations
17. Evaluate and communicate deficiencies
How Update Clarifies Requirements for Effective Internal Control – a final word before we go

• Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  • Each component and each relevant principle is present and functioning
  • The five components are operating together in an integrated manner

• Each principle is suitable to all entities; all principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component (e.g., governance, technology)

• Components operate together when all components are present and functioning and internal control deficiencies aggregated across components do not result in one or more major deficiencies
QUESTIONS

Lealan Miller
Eide Bailly LLP
877 W. Main Street, Suite 800
Boise, Idaho 83702
208.383.4756
lmiller@eidebailly.com