Using the COSO Framework to Develop a Strong and Preventive Control Environment

Weaver Public Sector CPE Event
Speakers

**Alyssa G. Martin, CPA**
Dallas Executive Partner, Advisory Services

25+ years of public accounting experience, with a practice emphasis in risk management, internal audit, and business process improvement

**Dan Graves, CPA**
Senior Manager, Advisory Services

10+ years of public accounting experience, with a practice emphasis in risk management and assessment, internal audit, and process improvement consulting
Topics

- Overview – COSO 2013 Internal Control Integrated Framework
- Considering All Risks and Costs
- Focus on Fraud and IT
- Putting It Into Action
- Common Transaction Processing Areas
  - Purchase-to-Pay
- Balancing Internal Controls
COSO Internal Control Integrated Framework
COSO Framework

COSO (Committee of Sponsoring Organizations) is an integrated framework for internal control which, when implemented, can provide a baseline to establish a control structure.

• COSO identifies five components of control that need to be in place and integrated into the organization’s operations

• The focus for a financial statement audit is on financial reporting

• Internal audit includes compliance and operations with financial reporting
What is Internal Control?

A process effected by an entity’s commissions or council, management and other personnel and designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding of assets
Requirements for 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

• A major deficiency represents an internal control deficiency or combination thereof that severely reduces the likelihood that an entity can achieve its objectives
<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>PRINCIPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrates commitment to <strong>integrity</strong> and <strong>ethical values</strong></td>
</tr>
<tr>
<td></td>
<td>2. Board is <strong>independent</strong> and oversees internal controls</td>
</tr>
<tr>
<td></td>
<td>3. Establishes <strong>structure</strong>, <strong>authority</strong> and <strong>responsibility</strong></td>
</tr>
<tr>
<td></td>
<td>4. Attracts, develops and retains <strong>competent individuals</strong></td>
</tr>
<tr>
<td></td>
<td>5. Holds individuals <strong>accountable</strong> for responsibilities</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>6. <strong>Specifies</strong> suitable and clear <strong>objectives</strong></td>
</tr>
<tr>
<td></td>
<td>7. <strong>Identifies</strong> and <strong>analyzes</strong> risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses potential for <strong>fraud risk</strong></td>
</tr>
<tr>
<td></td>
<td>9. <strong>Identifies</strong> and <strong>analyzes</strong> significant <strong>change</strong> and its impact</td>
</tr>
<tr>
<td>Control Activities</td>
<td>10. <strong>Selects</strong> and <strong>develops control</strong> activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops <strong>general controls</strong> over <strong>technology</strong></td>
</tr>
<tr>
<td></td>
<td>12. Deploys <strong>control activities</strong> through <strong>policies</strong> and <strong>procedures</strong></td>
</tr>
<tr>
<td>Information &amp;</td>
<td>13. Uses relevant, <strong>quality information</strong></td>
</tr>
<tr>
<td>Communication</td>
<td>14. Communicates <strong>internally</strong> internal control responsibilities</td>
</tr>
<tr>
<td></td>
<td>15. Communicates <strong>externally</strong> matters affecting controls</td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>16. Conducts ongoing and/or separate <strong>evaluations</strong> of controls</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates <strong>deficiencies</strong> to responsible parties</td>
</tr>
</tbody>
</table>
Considering All Risks and Cost
Risk Considerations

• Misappropriation of assets
• Fraudulent or inaccurate financial reporting
• Operational effectiveness and efficiency
• Compliance risk
• Reputational risk
• Regulatory and legal compliance risk
• Strategy and operational alignment
Risk Considerations

Balancing is important in both big and small organizations.

A number of studies support the conclusion that material weaknesses in internal control are more likely in smaller, younger and financially weaker organizations.
Targeted Process

Focus on driving standardization, and perfecting individual compliance activities:

• Improvements in upstream business processes

• Higher levels of maturity in overall compliance efforts
Internal Control Costs

- **Direct Costs**
  - Personnel
  - Third-party audits
  - IT systems

- **Indirect Costs**
  - Potential inefficiency
  - Reduced productivity
External Drivers

• COSO 2013
• State or Federal Audits and Reviews
• State or Federal Laws & Regulatory Guidance
• Federal Awards
Focus on Fraud and IT
Due to the advancement and sophistication of IT systems and the proliferation of fraudulent activity since the 1992 framework, the new COSO has an enhanced focus on IT and fraud considerations.
Assessing the significance of IT systems in your environment receives specific focus in the new COSO.

- Organization are encouraged to identify the significant systems within their environment and develop specific controls over the management and application of those systems.

- Additionally, organizations are challenged to consider their internal IT operations to ensure they have adequate authority, staffing, training, and expertise.

- Knowing your dependence on specific systems to operate and execute daily functions is a requirement to assessing the IT environment.

- Organization are encouraged to perform risk assessments to identify the likelihood and impact of fraud schemes in their environment.

- Requires the consideration of the three major components of committing a fraud – pressure, opportunity, and rationalization.

- An organization should know where they are vulnerable to different types of fraud and design controls to prevent and detect inappropriate activities.
Fraud Prevention: Why it Matters

- A typical organization loses 5% of its annual revenue to fraud
  - For 2014 GWP, this figure translates to a potential total fraud loss of more than $3.7 trillion

- The median loss caused by occupational fraud cases is $145,000
  - More than 22% of fraud cases involved losses of at least $1 million

- Fraud typically lasts a median of 18 months before being detected
The Fraud Diamond

Opportunity
Opens the door for the perpetrator

Incentive
Leads the perpetrator to the door

Rationalization
Coaxes the perpetrator to the door

Capability
Enables the perpetrator to walk through the door
Fraud Prevention: Detecting Occupational Fraud

Source: 2014 Association of Certified Fraud Examiners “Report to the Nation.”

“Other” category was not included in the 2010 Report.
## Top Fraud Scenarios

<table>
<thead>
<tr>
<th>Process</th>
<th>Fraud Scheme</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Revenue</td>
<td>• Improper/early revenue recognition&lt;br&gt;• Fictitious revenue</td>
<td>• Implement month-end review of financial statements&lt;br&gt;• Require review and approval of journal entries</td>
</tr>
<tr>
<td>2. Expenses</td>
<td>• Hiding losses in future reporting periods</td>
<td>• Implement month-end review of financial statements</td>
</tr>
<tr>
<td>3. Cash and Cash Equivalents</td>
<td>• Larceny&lt;br&gt;• Defalcation</td>
<td>• Establish ACH deposit into main operating account&lt;br&gt;• Implement lockbox through independent bank</td>
</tr>
<tr>
<td>4. Occupational Injury</td>
<td>• Non-compliance with FMLA, abuse of FMLA</td>
<td>• Require review and approval of submitted forms</td>
</tr>
<tr>
<td>5. Financial Reporting</td>
<td>• Manipulation of management estimates for receivables, goodwill, or depreciation</td>
<td>• Review and approval of journal entries&lt;br&gt;• Require supporting documentation for all estimates</td>
</tr>
<tr>
<td>6. Improper Note Disclosure</td>
<td>• Omission of material contingencies</td>
<td>• Implement month-end checklist reviewed by various members of management</td>
</tr>
<tr>
<td>7. Hiring Process</td>
<td>• Payment to fictitious employees</td>
<td>• Segregation of duties in the payroll process; outsource payroll</td>
</tr>
<tr>
<td>8. Compliance with contracts</td>
<td>• Awarding contracts to parties related to individuals involved in the decision making process</td>
<td>• Involve various members of management in contract approval; require two signatures for approval of material contracts</td>
</tr>
<tr>
<td>9. Assets</td>
<td>• Improper valuation of securities, inventory, fixed assets</td>
<td>• Management review and approval of valuation methods</td>
</tr>
<tr>
<td>10. Expense reimbursement process</td>
<td>• Reimbursement for undocumented expenses</td>
<td>• Require employee expense reimbursement forms with attached original receipts</td>
</tr>
<tr>
<td>11. Competitive Bid Rigging</td>
<td>• Establishing criteria that gives select vendors an unfair advantage</td>
<td>• Require independence confirmation for all members involved in negotiations</td>
</tr>
<tr>
<td>12. Performance and Compensation Review</td>
<td>• Overpayment to existing employees</td>
<td>• Segregation of duties in the payroll process; outsource payroll</td>
</tr>
<tr>
<td>13. Credit Card Process</td>
<td>• Reimbursement for personal, non-deductible expenses</td>
<td>• Require employee acceptance of Terms of Use and re-payment for personal expenses</td>
</tr>
<tr>
<td>14. Non-Financial</td>
<td>• Falsifying external documents to suppliers</td>
<td>• Require approved contracts and purchase orders</td>
</tr>
<tr>
<td>15. Document Storage</td>
<td>• Destruction or disappearance of records</td>
<td>• Establish Code of Conduct that restricts tampering with records; third-party document storage</td>
</tr>
</tbody>
</table>

### Fraud Scheme Response

- Implement month-end review of financial statements
- Require review and approval of journal entries
- Implement lockbox through independent bank
- Require independence confirmation for all members involved in negotiations
- Segregation of duties in the payroll process; outsource payroll
- Require employee expense reimbursement forms with attached original receipts
- Require approved contracts and purchase orders
- Establish Code of Conduct that restricts tampering with records; third-party document storage
The Framework in Action: Assessing & Designing Internal Controls
Assessing Internal Controls

• Are your controls keeping pace with your organization?
  – Major change - your growth, changes in programs, restructurings, or new markets, products, and partners introduce risk

• Changes in the operating environment
  – Accelerating pace of operations - Your controls need to adapt to planned changes and unforeseen circumstances and keep in sync with the organization
  – New and evolving expectations for non-financial reporting - stakeholders seek greater transparency and confidence in your reporting
  – Ongoing regulatory oversight and scrutiny

• Changes inside the organization
  – Greater complexity in your operating model and structure
  – Complex, interconnected operations
  – Expanding reliance on technology - new uses of existing technology and new investments may impact risks for internal and external interactions
How effective is your internal control?

- Do your strategic goals, initiatives, priorities, or operating decisions introduce new risks that impact your internal control?
- Should we consider additional opportunities for applying internal control to important reporting, operations, and compliance objectives? Why not?
- What breakdowns have we experienced with existing controls? Why didn’t we know about those before? How could they have been prevented?
- Do internal controls reduce identified risks to an acceptable level?

How do your entity-level controls map to each of the principles?

- Follow the points of focus
- Cover each attribute
- Evaluate the coverage of your entity-level controls
- Provide a baseline on which to build process-specific controls
COSO 2013 Internal Control Framework Mapping

Mapping describes how various controls affect COSO Principles.

<table>
<thead>
<tr>
<th>Component</th>
<th>Control Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle</td>
<td>1. The organization demonstrates a commitment to integrity and ethical values.</td>
</tr>
</tbody>
</table>

- **Controls embedded in other principles or components that may affect the principle**
  - **Control Environment**: Human Resources review employees’ confirmations to assess whether standards of conduct are understood and adhered to by staff across the entity.
  - **Information & Communication**: Management obtains and reviews data and information underlying potential deviations captured in whistle-blower hotline to assess quality of information.
  - **Monitoring Activities**: Internal Audit separately evaluates Control Environment, considering employee behaviors and whistle-blower hotline results and reports thereon.
## COSO 2016: Control Activities

The policies and procedures that help ensure that management directives are carried out. They take many forms including policies and procedures, approvals, verifications, reconciliations, performance reviews, security measures, and segregation of duties.

<table>
<thead>
<tr>
<th>Control Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. The organization <strong>selects and develops control activities</strong> that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</td>
</tr>
<tr>
<td>11. The organization <strong>selects and develops general control activities</strong> over technology to support the achievement of objectives.</td>
</tr>
<tr>
<td>12. The organization <strong>deploys control activities through policies</strong> that establish what is expected and procedures that put policies into place.</td>
</tr>
</tbody>
</table>
**Nature of Controls: Preventive vs. Detective**

**Preventive Controls:** Either people-based or systems-based, designed to prevent errors or omissions (including fraud) from occurring and are generally positioned at the source of the risk within a business process.

- Standards, policies and procedures are the most basic type of preventive controls.
- Segregation of duties also acts as a preventive control against fraud.
- Authorization/approval levels also prevent the risk of an illegal act and are thus preventive in nature.

**Detective Controls:** Either people-based or systems-based, designed to detect and correct errors or omissions (including fraud) within a timely manner prior to completion of a stated objective.

- Exception reports – review of various exception reports helps in detecting errors.
- Reconciliations – after the fact reconciliations act as a double check against errors and exceptions.
- Periodic audits also act as a very good detective control.
Nature of Controls: Primary vs. Secondary

**Primary Controls**
- Controls that are especially critical to the mitigation of risk and the ultimate achievement of one or more financial reporting assertions for each significant account balance, class of transactions and disclosure
- Controls that managers and process owners primarily rely on

**Secondary Controls**
- Controls important to the mitigation of risk and the ultimate achievement of one or more financial reporting assertions, but are not considered “critical” by management and process owners
- These controls are significant, but there are compensating controls that also assist in achieving the assertions
Designing Effective Internal Control Activities

• **Understanding the Risk**
  – In order to identify appropriate control activities the risks inherent in a particular process or organization must be identified.

• **Identifying Control Activities**
  – Once you have identified the risk, identify the control activity, reducing the identified risk to an acceptable level.
  – The controls identified to reduce risk may be direct and precise.
  – Each identified risk should have a primary control or a group of secondary controls that appropriately mitigate those risks.
Effective Internal Control Activities

• Recommendations for Design Improvement
  – Compare Benefit vs. Costs
    • Consider People, Process, Technology
    • Example: There is no point in protecting an asset worth a couple of hundred dollars with a biometric control costing thousands.
  – Establish Internal Control
    • Identify and establish activities as internal controls
    • Define purpose, frequency, documentation
  – It is management’s responsibility to evaluate the design and determine if the risk is acceptable.
## Purchase-to-Pay: Identify the Relevant Risks

### Purchasing

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Purchases are recorded into the general ledger completely and accurately when received.</td>
</tr>
<tr>
<td>2</td>
<td>Open purchase orders received are recorded in the general ledger.</td>
</tr>
<tr>
<td>3</td>
<td>Bids and purchases are approved by authorized personnel.</td>
</tr>
<tr>
<td>4</td>
<td>Coding of bids and purchases is correct.</td>
</tr>
<tr>
<td>5</td>
<td>Fictitious or duplicate vendors are not set up and purchases are not recorded.</td>
</tr>
<tr>
<td>6</td>
<td>Purchases are correctly capitalized.</td>
</tr>
<tr>
<td>7</td>
<td>Purchase contracts are authorized and do not contain kickback arrangements.</td>
</tr>
<tr>
<td>8</td>
<td>Open purchase orders are tracked to ensure that they are filled by vendors.</td>
</tr>
</tbody>
</table>

### Accounts Payable

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Purchases/payables are recorded and coded correctly.</td>
</tr>
<tr>
<td>10</td>
<td>Invoices represent goods/services actually received.</td>
</tr>
<tr>
<td>11</td>
<td>Fictitious or duplicate invoices are not recorded.</td>
</tr>
<tr>
<td>12</td>
<td>Invoices reflect correct prices, quantities and other valuation information.</td>
</tr>
<tr>
<td>13</td>
<td>PO variances with the vendor invoice is approved by authorized personnel.</td>
</tr>
<tr>
<td>14</td>
<td>Vendor invoices are properly authorized.</td>
</tr>
<tr>
<td>15</td>
<td>Only authorized employees are allowed to use District credit cards.</td>
</tr>
</tbody>
</table>

### Cash Disbursements

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Cash disbursements are correctly coded.</td>
</tr>
<tr>
<td>17</td>
<td>Cash disbursements are recorded in the proper period.</td>
</tr>
<tr>
<td>18</td>
<td>Cash disbursements are recorded when paid.</td>
</tr>
<tr>
<td>19</td>
<td>Cash disbursements relate to actual purchases/expenses.</td>
</tr>
<tr>
<td>20</td>
<td>Duplicate or fictitious cash disbursements are not processed.</td>
</tr>
<tr>
<td>21</td>
<td>Cash disbursements are properly authorized.</td>
</tr>
<tr>
<td>22</td>
<td>Cash disbursement amounts recorded agree with amounts paid.</td>
</tr>
</tbody>
</table>

Consider the related subprocesses that make up the overall cycle or process area being evaluated. In Purchase-to-Pay, that includes:

- Procurement
- AP
- Disbursements

These all have their own unique risks.
Purchase-to-Pay: Identify the Controls

**AUTHORIZATION AND SEGREGATION OF DUTIES**

- The organization has established **delegation of authority** to indicate the value and type of expense that may be approved by each individual.

- Purchase orders and invoices are routed for **approval** based on the authority limits established in the system. Authorization is required for issuing a PO or recording an invoice.

- Purchasing issues POs and tracks status. AP receives invoices and records transactions. Individuals do not have **access** to Purchasing and AP.
Purchase-to-Pay: Identify the Controls

**PROCESSING AND MATCHING**

- Invoices are *matched* to a Purchase Order and receiving document upon receipt by the AP department.

- AP codes each invoice and submits it for approval based on the *approval* routing established in the system. Approvers sign off on invoices electronically to indicate that the goods were received in good condition, the value is accurate, and the coding is appropriate.

**DISBURSEMENT TYPE**

- Manual checks are requested on a check form and *approved* by the CFO.

- Wire disbursements are requested on a wire form and *approved* by the CFO. The Controller sets up wires on the bank portal and the CFO releases.
Purchase-to-Pay: Evaluate Control Design

**Do the control activities for a given process contain a sufficient quantity of preventive and detective controls?**

A well designed control environment contains a mix of preventive and detective controls. We frequently see a tendency to rely on detective controls, as opposed to leveraging system functionality to build preventive controls into the process.

<table>
<thead>
<tr>
<th><strong>Detective Control</strong></th>
<th><strong>Complimentary Preventive Control</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Controller reviews the final check register to ensure that printed checks match the approved check run.</td>
<td>The Controller reviews the final check run and prepares the Positive Pay that is issued to the bank to authorize the printed checks.</td>
</tr>
</tbody>
</table>
Purchase-to-Pay: Linking Controls to COSO

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

**Points of Focus**
- Reflects External Laws and Regulations: Laws and regulations establish minimum standards of conduct which the entity integrates into compliance objectives.

**Control Activity**
- Purchase Order’s over $50,000 must include three formal bids and be approved by Council.
Balancing Internal Controls
Consider both **loss mitigation** and **cost mitigation** in recommending controls.

- Communicate the link between internal controls, risk management, and profitability.
- The costs of a control should never exceed the benefits of a control.
Balanced Controls

Establish efficient separation of duties
- Deploy minimal number of employees for processes

Increase reliance on system controls
- Limit posting and maintenance access
- Utilize auto-balancing capabilities
- Establish dual control
Focus on crucial issues

- Determine which activities pose greatest degrees of risk
- Ensure that secondary reviewers of critical activities consider:
  - Accuracy
  - Completeness
  - Validity
  - Reasonableness
Summary

The COSO 2013 Internal Control Integrated Framework is a comprehensive baseline for evaluating the adequacy of control at your organization.

- Leveraging the 17 principles to walk through and evaluate controls will help to ensure your controls are adequately designed.

Start by identifying and relying on entity level controls that span all process areas.

- Strong entity level controls provide a reliable foundation upon which to build process-specific control activities.

Process-level controls can be used to show coverage of certain principles and points of focus where entity-level controls are not highly specific or precise.

- Adequately designed process controls that are developed with the COSO principles in mind will ensure a streamlined and integrated control structure.
Questions

Thank You

Alyssa G. Martin
Partner, Risk Advisory Services
alyssa.martin@weaver.com

Dan Graves
Senior Manager, Risk Advisory Services
daniel.graves@weaver.com