COSO internal control framework as a best practice for utilities

June 2014

The most widely-used framework for internal control assessments is from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Many public companies also rely on the framework to assess the effectiveness of internal control over external financial reporting (ICEFR) under Sarbanes-Oxley (SOX) section 404.

While SOX may not apply to all utilities, this framework is a best practice in design of internal controls and following it can allow for a strong compliance framework to support strategic goals.

Three factors within COSO’s Internal Control-Integrated Framework make it easier to design and evaluate the effectiveness of internal control:

1. **Inclusion of internal control principles.** Seventeen principles explain concepts associated with the five internal control components. Each of the five components of internal control and relevant principles must be present and functioning.

2. **Consideration of business changes.** The framework includes guidance for assessing risk and updating related controls that consider how business may have changed, particularly through outsourcing of business processes and reliance on information technology.

3. **Beyond financial reporting.** Objectives are expanded beyond financial reporting, to include internal and non-financial external reporting.

**Overall Framework**

The overall COSO Framework has not changed. It states that an effective control structure is designed to address the following three objectives:

1. **A- Operations**- effective and efficient use of resources
2. **B- Reporting**- reliability of reporting
3. **C- Compliance objectives**- compliance with applicable laws and regulations

These objectives are met within the Framework through five components and seventeen principles as shown in the table on the next page.
Framework principles

<table>
<thead>
<tr>
<th>Control environment</th>
<th>Risk assessment</th>
<th>Control activities</th>
<th>Information and communication</th>
<th>Monitoring activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Demonstrates commitment to integrity and ethical values</td>
<td>6 Specifies suitable objectives</td>
<td>10 Selects and develops control activities</td>
<td>13 Uses relevant information</td>
<td>16 Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td>2 Exercises oversight responsibility</td>
<td>7 Identifies and analyzes risk</td>
<td>11 Selects and develops general controls over technology</td>
<td>14 Communicates internally</td>
<td>17 Evaluates and communicates deficiencies</td>
</tr>
<tr>
<td>3 Establishes structure, authority, and responsibility</td>
<td>8 Assesses fraud risk</td>
<td>12 Deploys through policies and procedures</td>
<td>15 Communicates externally</td>
<td></td>
</tr>
<tr>
<td>4 Demonstrates commitment to competence</td>
<td>9 Identifies and analyzes significant change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Enforces accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fundamental concepts remain similar to the 1992 original, but the updated framework released in 2013 also includes points of focus describing the characteristics that underlie each principle. These points are not required for assessing the effectiveness of internal control. However, management can use the points to design, implement, and evaluate internal controls. The points also help assess if relevant principles are present and functioning. The framework also explicitly considers potential sources of fraud when assessing risks to the achievement of an organization’s objectives. These sources include management override, safeguarding of assets, incentives, pressures, and opportunities for inappropriate acts, as well as attitudes and rationalizations that may justify these acts.

Transition
COSO has encouraged users to transition their application and related documentation to the updated framework as soon as is feasible, as the updated framework will supersede the original after December 15, 2014. During the transition period, COSO also suggests that any organizations reporting externally should clearly disclose whether the original or updated framework was utilized. As a result, when companies provide their annual assessment of ICEFR in accordance with SOX, the user should indicate which framework they used to perform the assessment.
Recommended approach for adopting the framework:

I. Review & understand changes to the framework
   - Assess training and education needs

II. Assess coverage of principles to existing processes, consider points of focus
   - Identify gaps from assessment

III. Discuss initiative and mapping results with leadership
   - Get support for compliance efforts
   - Educate stakeholders

IV. Determine steps to remediate identified gaps
   - Develop timeline to achieve compliance

V. Establish monitoring and oversight of implementation
   - Develop method and procedures to identify need for future changes

Many organizations that are not subject to SOX compliance have adopted the COSO Framework and 80% of SEC companies indicate they do follow the COSO Framework. It would be prudent for a utility to review its control environment to ensure proper controls are in place. In order to obtain strategic goals, a utility needs to have effective and efficient operations, a strong reporting and compliance framework, and the proper governance oversight in place supporting the strategy.

Connect with us today:

Russ Hissom, Partner
608 240 2361
russ.hissom@bakertilly.com