RELATING the COSO Internal Control—Integrated Framework and COBIT
Many enterprises ask, “With the update of both the COSO Internal Control — Integrated Framework and the COBIT framework, are they still complementary and compatible? The answer to this question is yes, the frameworks are complementary and compatible as guidance to support the assessment and improvement of internal control practices and activities within the governance and management arrangements of an enterprise.

BACKGROUND

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control — Integrated Framework and the ISACA COBIT framework have a long and beneficial history of in-tandem use by many enterprises, long before the Sarbanes-Oxley Act of 2002 regulations were enacted. With the advent of this set of regulatory challenges, enterprises were compelled to use COSO for their financial framework. (The U.S. Securities and Exchange Commission mentioned the COSO framework as one of the sources of guidance for evaluating internal control over financial reporting.) These same enterprises were also drawn to COBIT for their IT control framework guidance because of the specific IT Control Objectives for Sarbanes Oxley product that ISACA published and their recognition of IT as a critical enabler to the operation of strong financial controls. In May 2013, COSO released its updated and refreshed Internal Control — Integrated Framework. ISACA participated in this update program, serving as a member of the COSO Advisory Council. Meanwhile, ISACA released COBIT 5, its update and revision to COBIT, in April 2012. Because many enterprises rely on the use of both frameworks internally and many others use both frameworks in their consulting work, ISACA realized the natural need to consider how the two frameworks relate to each other. For this reason, ISACA developed this white paper to present the ISACA perspective on the relationship between the two frameworks and to support dialogue among professionals who use the frameworks.

This article takes the refreshed and updated COSO Internal Control — Integrated Framework as its base structure and examines how the relevant components and content of the COBIT 5 framework and its supporting guidance deliverables relate to the COSO framework. Through the efforts of many (including ISACA), the May 2013 refreshed COSO framework places much stronger emphasis on the importance of information technology, in addition to other enhancements within its principles. The purpose of this article is to highlight areas of alignment and differences in the content of the frameworks, and also to help enterprises that are using the COSO framework by presenting the relationship between the COSO framework guidance and the COBIT 5 framework guidance. (It is assumed that readers have an understanding of the COSO and COBIT 5 framework concepts and components, which are freely available in foundational reference publications, on each organization’s website. Therefore, the repetition of content from these reference publications is kept to a minimum.)

THE COSO INTERNATIONAL CONTROL — INTEGRATED FRAMEWORK

(Note: This section quotes directly from the COSO International Control — Integrated Framework.)

The framework assists management, boards of directors, external stakeholders, and others interacting with the entity in their respective duties regarding internal control without being overly prescriptive. It does so by providing both understanding of what constitutes a system of internal control and insight into when internal control is being applied effectively.

Internal control is defined as follows:

Internal control is a process, affected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

This definition reflects certain fundamental concepts. Internal control is:

- Geared to the achievement of objectives in one or more categories — operations, reporting, and compliance
- A process consisting of ongoing tasks and activities — a means to an end, not an end in itself
- Effected by people — not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to provide reasonable assurance — but not absolute assurance, to an entity’s senior management and board of directors
- Adaptable to the entity structure — flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

COBIT 5: BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT.

COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, encompassing the full end-to-end business and IT functional areas of responsibility and consider-

<table>
<thead>
<tr>
<th>Exhibit 1: COSO Related to COBIT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO Framework Concept</td>
</tr>
<tr>
<td>Objectives</td>
</tr>
<tr>
<td>Process</td>
</tr>
<tr>
<td>People</td>
</tr>
<tr>
<td>Reasonable assurance</td>
</tr>
<tr>
<td>Adaptable</td>
</tr>
</tbody>
</table>
ing the IT-related interests of internal and external stakeholders. COBIT 5 uses enablers, which are broadly defined as anything that can help to achieve the objectives of the enterprise. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT defines seven categories of enablers.5

How COSO Framework Fundamental Concepts Relate to COBIT 5 Framework Components and Content

Exhibit 1 summarizes the relationship of COBIT 5 framework components with the fundamental concepts of the COSO framework.

COSO FRAMEWORK RELATIONSHIP OF OBJECTIVES AND COMPONENTS

The COSO framework comprises three dimensions — the objectives, components, and organizational structure of an entity — in a cube model, as illustrated in Exhibit 2.

COBIT 5 FRAMEWORK RELATIONSHIP OF COMPONENTS AND CONTENT

The COSO Internal Control — Integrated Framework provides a sound basis from which to establish and assess internal control arrangements, using the model in Exhibit 2, to integrate its dimensions. Likewise, the COBIT 5 framework provides a sound basis from which to establish, improve, and assess GEIT arrangements, based on the following four key models, shown in Exhibits 3 through 6.
- **Value Creation** — The overall COBIT governance objective (see Exhibit 3).
- **Five COBIT 5 principles** (see Exhibit 4).
- **Goals** based on the Kaplan and Norton Balanced Score Card — Financial, Customer, Internal, and Learning and Growth cascade with business goals, IT-related goals and enabler goals (see Exhibit 5).
- **Seven supporting enabler types** (see Exhibit 6).

**COSO FRAMEWORK OBJECTIVES**

The framework provides for three categories of objectives, which allow organizations to focus on differing aspects of internal control:

- **Operations Objectives.** These pertain to effectiveness and efficiency of the entity’s operations, including operational and financial performance goals, and safeguarding assets against loss.
- **Reporting Objectives.** These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity’s policies.
- **Compliance Objectives.** These pertain to adherence to laws and regulations to which the entity is subject.⁷

**COBIT 5 also focuses on enterprise objectives (referred to as goals), through the use of the goals cascade model. As shown in Exhibit 5, the goals cascade includes enterprise, IT-related and enabler goals. The generic goals provided in the COBIT 5 guidance, for adoption by enterprises, are based on the four dimensions of the balanced scorecard.⁸ These dimensions, in turn, relate to the enterprise benefits realiza-**

**Exhibit 5: COBIT 5 Goals Cascade**

Note: Enablers are factors that, individually and collectively, influence whether something will work — in this case, governance and management over enterprise IT.
ation, risk optimization, and resource optimization objectives, which can be aligned with the COSO framework operations, reporting, and compliance objectives.

The COBIT 5 framework relates to the COSO framework categories of objectives, as follows:

• **Operations.** COBIT is widely accepted as a best practice for governance and management of IT-related processes.

• **Reporting.** The COBIT 5 goals cascade and MEA domain processes support the COSO framework reporting objective category.

• **Compliance.** The COBIT 5 process MEA03 external compliance-focused process, and the COBIT 5 alignment with several relevant standards and frameworks support the COSO framework Compliance objective category. COBIT is used as the basis for internal/external audits and regulatory guidance in certain locations and industries.

The 17 generic enterprise goals that are defined in COBIT 5 (Exhibit 7) cover all aspects of operations goals across the four balanced scorecard dimensions. Enterprise reporting goals include financial transparency and information-based strategic decision making. Enterprise compliance goals include compliance with external laws and regulations and with internal policies.

**COSO FRAMEWORK PRINCIPLES AND COMPONENTS**

“The framework sets out 17 principles representing the fundamental concepts associated with each component. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all principles. All principles apply to operations, reporting, and compliance objectives.”

**CONCLUSION**

This article provides a high-level explanation of how the two widely used frameworks align and the value of using COSO and COBIT together.
The COSO framework provides useful principles on internal control; the COBIT 5 framework provides additional guidance on the information- and technology-related governance and management enablers that are critical to the operation of internal financial controls in enterprises. ISACA anticipates additional thinking regarding the benefits and usefulness of both frameworks and looks forward to observing further discussions about how enterprises are using these two globally accepted frameworks together.

Additional information about COSO and how to obtain the framework can be found at the COSO web site, www.coso.org/ic.htm. Likewise, the COBIT framework and supporting guidance, training materials and sources can be found at the COBIT web site www.isaca.org/COBIT.

**Exhibit 7: COBIT 5 Enterprise Goals**

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Goal</th>
<th>Benefits Realization</th>
<th>Risk Optimization</th>
<th>Resource Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>1. Stakeholder values of business investment</td>
<td>P</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>2. Portfolio of competitive products and services</td>
<td>P</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>3. Managed business risk (safeguarding of assets)</td>
<td>P</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>4. Compliance with external laws and regulations</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Financial transparency</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>Customer</td>
<td>6. Customer-oriented service culture</td>
<td>P</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>7. Business service continuity</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Agile responses to a changing business environment</td>
<td>P</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>9. Information-based strategic decision making</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>10. Optimization of service delivery costs</td>
<td>P</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>Internal</td>
<td>11. Optimization of business process functionality</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Optimization of business process costs</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. Managed business change programs</td>
<td>P</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>14. Operational and staff productivity</td>
<td>P</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>15. Compliance with internal policies</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learning and Growth</td>
<td>16. Skilled and motivated people</td>
<td>S</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>17. Product and business innovation culture</td>
<td>P</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key:  P = Primary,  S = Secondary

Source: ISACA, COBIT 5, 2012, Exhibit 5

**Notes**

5. ISACA.
7. Ibid.
8. Kaplan.
9. Relevant standards include the International Organization for Standardization (ISO)/International Electrotechnical Commission 27000 series, and relevant frameworks include The Open Group Architecture Forum 9 and Information Technology Infrastructure Library V3.
10. COSO May 2013.