COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2022
Effective compliance programs require top-down internal controls

By Deena King and Marisa Zuskar

Deena King (deenaking@uttyler.edu) is the author of Compliance in One Page and the forthcoming Strategic Compliance, and is a Chief Compliance Officer at The University of Texas at Tyler in Tyler, Texas, USA. **Marisa Zuskar** (mzuskar@hcg.com) is a Senior Director at Chicago-based Huron Consulting Group.

Deena King

Marisa Zuskar

We recently read two columns on internal controls, one by Joe Murphy and the other by SCCE & HCCA CEO Gerry Zack, in the November 2021 issue of *CEP Magazine*. These pieces resonated with us, because we, the authors, are passionate about the positive impact of internal controls in strengthening compliance programs and have spoken together on this issue at a couple SCCE events.[1]

In his column, Murphy shared some concerns about the use of internal controls in compliance programs and raised several valid examples of how internal controls, when not "approached thoughtfully" can be detrimental to an organization's environment.[2] He added that they can sometimes "appear oppressive" and lead employees to willfully work around compliance controls meant to protect the organization (which can make many compliance professionals nervous). In the second column we read, Zack stated, "Internal controls over compliance are the foundation of any compliance program," conceding that internal controls should be carefully reviewed to ensure they are reasonably designed and effective.[3]

We, the authors, have our own biases related to this topic, which can be summed up in the following statement: Laws/regulations + internal controls = effective compliance.[4]

In our view, what makes the compliance profession so unique is the yin-yang-like collaboration that must occur between regulatory experts and internal controls specialists. Regulatory experts are focused on all the legal requirements and laws affecting an entity while internal controls specialists have expertise in operationalizing these laws via compliance programs within other business functions.

We hope that Murphy agrees with the following idea—that the objective of compliance programs is to achieve operational alignment with the requirements that come from a large body of laws and regulations.

As compliance leaders, the body of laws we care about are going to be dictated by our industry—healthcare, finance, energy, utilities, higher education, etc. Understanding the laws and regulations relevant to our industries, therefore, is necessary to the design and implementation of an effective compliance program and its elements, including policy, organizational design, procedure, communication, and training.

The Federal Sentencing Guidelines *and* internal controls

We also firmly believe that *any effective* compliance program must incorporate internal controls—from top to

bottom.

In his column, Murphy seems to suggest that internal controls, at least in the Federal Sentencing Guidelines (FSG) perspective,[5] are specifically intended to prevent and detect criminal conduct. However, when it comes to internal controls, the goals and objectives are much broader. Internal controls also include the mechanisms, rules, and procedures designed to promote federal compliance and adherence to laws and regulations.[6]

The oft-discussed FSG on effective compliance and ethics programs provides our first piece of evidence that internal controls are a necessary top-down compliance program element. These guidelines are only two pages long, and despite the regular reducing of the FSG to seven elements, they contain 17 "shalls." And notwithstanding the specific reference to internal controls cited by Murphy,[7] *most of these "shalls" are internal controls*. Yes, you read that right.

Internal controls form the framework necessary to convert all those laws and regulations into compliance programs. As Zack said, "It's not a stretch to say that every compliance program comprises a complex assortment of preventive and detective internal controls, some of which are general in nature…while others are specific and more granular in nature."[8]

The COSO internal controls framework

To help the reader understand our confidence in the assertion that internal controls are a must-have for any compliance program to be effective, we introduce our second piece of evidence—the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control - Integrated Framework*. COSO is the author of the widely accepted definition, framework, and guidance related to internal controls. As defined by COSO, an internal control is "a process, effected 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."[9]

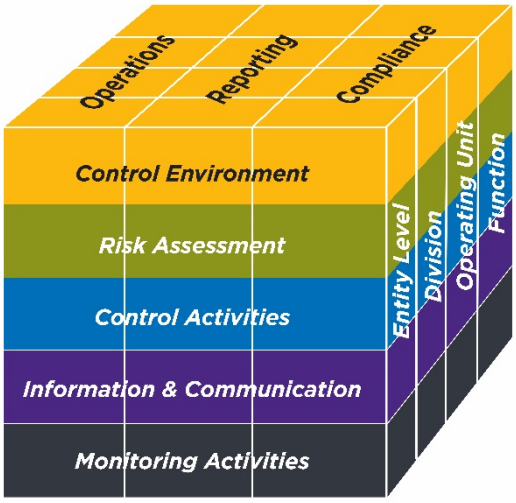
COSO highlights a clear connection between achieving compliance and internal controls because internal controls are the tactical tools that help organizations achieve objectives *related to compliance*. Thus, COSO is offering us a framework of interrelated, cross-dependent tactical tools that have proven effective in promoting compliance. Zack and Murphy agree—it is impossible to make an organization 100% compliant or "noncompliance-proof." However, we postulate that with a diverse and integrated system of internal controls to ensure there is no one person or point of weakness, an organization can reach that goal of "reasonable assurance."

And *all* these controls are represented in the FSG.

COSO cube *and* the seven elements

A summary of the high-level internal controls structure that COSO recommends can be found on the face of what is often called the "COSO cube" (Figure 1).

Figure 1: The COSO cube



The components of internal control (or activities of compliance) are:

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring Activities

Where internal controls need to be implemented can be found on the side of the cube, which represents the layers of an organization:

- Entity Level
- Division
- Operating Unit
- Function

Some of the items on these lists should sound familiar, as there is clear overlap and alignment between the seven elements and FSG. For example, the side of the cube defines the top-down macro and micro levels of the organization where controls are implemented. This is analogous to USSG § 8B2.1(b)(2), where three general levels of personnel have a duty to be engaged in compliance responsibilities ("shall be delegated"): the governing authority (Entity Level), high-level personnel (Entity Level), and specific individual(s) (Division/Operating Unit/Function).

Both the seven elements and FSG are clearly represented on all three faces of the COSO cube. Many compliance

professionals believe that the seven elements are just useful program guidance, but what they may not yet understand is that the FSG represent a federal regulatory duty for entities to implement effective internal controls as detailed on the front of the COSO cube. The FSG states that compliance programs "shall" have these controls, and these controls "shall" be implemented organization-wide, as detailed on the side of the cube.

Table 1 illustrates how each of the seven elements aligns with the front and side of the COSO cube guidance on internal controls (i.e., how *each* of the seven elements represent *distinct* internal controls as defined by COSO).

FSG Element[10]	COSO Internal Control — Integrated Framework
Standards of conduct, policies, procedures	• **Front: Control Activities**
Compliance officer and committee(s)	• Side: Entity level, Division, Operating Unit, Function
Communication and education	• **Front: Information and Communication**
Internal monitoring and auditing	• Front: Monitoring Activities
Reporting and investigating	• Front: Control Activities • Top: Reporting
Enforcement and discipline	• Front: Control Activities
Response and prevention	• Front Monitoring Activities *(that lead to improvements)*

Table 1: The FSG seven elements compared to the COSO cube

Note: Bolded items will be the focus of case study examples in the next section.

You may have noticed that there are two missing COSO components. Though Assess Risk and Organizational Culture are not included in many "official" seven elements lists, these requirements are inherent in the FSG (USSG § 8B2.1(c) and 8B2.1(a)(2), respectively), so they are often incorporated into compliance programs.

Applying compliance internal controls in real life

In Tables 2 and 3, we look at a case study focusing on conducting background checks for new hires that defines the organizational responsibilities (cube side). Because a point-by-point discussion on how to implement all

control components across each level of the entity and how these fit into the institution's unique compliance environment would require a much lengthier article, we will limit our examples to two COSO controls and the corresponding seven elements control where applicable:

- **COSO:** Control activities, and **FSG:** Standards of conduct, policies, and procedures; and
- **COSO:** Information and communication, and **FSG:** Communication and education.

Level (COSO Side)	Compliance Responsibility		Internal Control Example
Entity	Standard and Policy Management	Responsible for designing and implementing organization-wide standards, policies, and procedures	Implementing and maintaining a policy that requires background checks for all new hires
Division	Division Policy and Process Management	Responsible for designing and implementing division-level policies and procedures	Human resources implements a process, including forms, that includes a required background check for all new hires with logs
Functions	Follow the policy and use the process	Responsible for following policy and using procedures	All new hires will complete the appropriate paperwork and submit themselves to a background check, as needed

Table 2: COSO Control Activities: FSG Standards of Conduct, Policies, and Procedures

Level (COSO Side)	Compliance Responsibility		Internal Control Example
Entity	Corporate Training and Communication	Responsible for designing and implementing a communication and training plan for the entire organization	Organization-wide training informs all employees at least annually that background checks are conducted for all new hires
Division	Division Communications	Responsible for designing and implementing division-level communication and training	During the recruitment process, human resources informs all new candidates that background checks will be required for all new hires

Functions	Follow the policy and use the process	Submit to a background check	Provide all the required information to allow for a successful background check

Table 3: COSO Information and Communication: FSG Communication and Education

This exercise can be repeated to design additional operational and functional controls across the cube sides (e.g., review and approval of new vendors, mandatory vacations). Almost all operational and functional controls of this type will originate and build upon a top-down entity-level control; that is, a culture of compliance has the highest impact on day-to-day compliance.

The right combination

While effective compliance certainly can't exist without laws and regulations, it also cannot exist without top-down internal controls, a viewpoint supported by both the FSG and COSO. The combination of the laws that define the outcome-focused requirements of an organization alongside a custom program of diverse internal controls is what makes our profession unique and what requires the yin-yang-like collaboration and balance mentioned at the beginning of this article. Really good compliance requires effective, ongoing collaboration between regulatory experts to review and interpret the law and its requirements and internal controls specialists to effectively implement the framework in balance with other operational goals (e.g., efficiency, financial viability).

Understanding how to apply internal controls to compliance as recommended by COSO (i.e., COSO's*Internal Control – Integrated Framework*) and the FSG will help our compliance programs be more effective and efficient.

Takeaways

- Effective compliance programs are based on laws and regulations and associated internal controls.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework* provides excellent guidance that supports effective compliance.
- The seven elements of an effective compliance program are represented on all sides of the COSO cube.
- The Federal Sentencing Guidelines include 17 "shalls," many of which are internal controls.
- Understanding how to apply internal controls to our compliance programs will support effectiveness and efficiency.

1 Marisa Zuskar and Deena King, "Who's Afraid of Internal Controls? Not me! Using Internal Controls to Make Higher Education Compliance Programs More Effective," Higher Education Compliance Conference, Society of Corporate Compliance and Ethics, June 2, 2020, https://compliancecosmos.org/whos-afraid-internal-controls-not-me-using-internal-controls-make-higher-education-compliance-0; Marisa Zuskar and Deena King, "Who's Afraid of Internal Controls? Not Me! Using Internal Controls to Manage Risk and Make Compliance Programs More Effective," Compliance and Ethics Institute, Society of Corporate Compliance and Ethics, September 22, 2021, https://compliancecosmos.org/whos-afraid-internal-controls-not-me-using-internal-controls-manage-risk-and-make-compliance-0.
2 Joe Murphy, "Do 'internal controls' belong in compliance programs?" *CEP Magazine*, November 2021,

https://compliancecosmos.org/do-internal-controls-belong-compliance-programs.
3 Gerry Zack, "Internal controls—the tools of compliance," *CEP Magazine*, November 2021, https://compliancecosmos.org/internal-controls-tools-compliance.
4 Deena King, *Compliance in One Page*, *Second Edition* (December 2020). All rights reserved. Used with permission.
5 USSG § 8B2.1 (U.S. Sentencing Comm'n 2018).
6 USSG § 8B2.1(b)(6).
7 USSG §8B2.1 Comm. 1.
8 Zack, "Internal controls—the tools of compliance."
9 Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, May 2013, https://www.coso.org/Pages/default.aspx.
10 "7 Elements of an Effective Compliance & Ethics Program," Society of Corporate Compliance and Ethics, accessed February 2, 2022, https://assets.corporatecompliance.org/Portals/1/PDF/Resources/CCEW/2021-ccew-7-elements-poster-for-web-8.5x11.pdf.