August 4, 2017

Integrating a Compliance & Ethics Program with a Control Framework
Leveraging COSO's *Internal Control – Integrated Framework*

By Ron Kral, CPA, CMA, CGMA
Member of Candela Solutions LLC

While many organizations have a compliance and ethics program (Program) to prevent and detect criminal conduct, some struggle to weave it into their culture to best protect themselves. A starting point is to thoroughly understand minimum requirements as defined in Chapter 8, Part B of the U.S. Sentencing Guidelines (Guidelines) entitled *Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program* published by the U.S. Sentencing Commission. The Guidelines provide incentives to organizations that follow a structural foundation to self-police their own conduct through an effective Program. Next is to integrate the Program requirements into a control framework, such as the *Internal Control – Integrated Framework* of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Finally, the Program's expectations and controls need to be entrenched into the cultural fabric of the organization. This article offers an approach in addressing the Guideline's minimum requirements in harmony with COSO's *Internal Control – Integrated Framework* (COSO Framework).

Minimum Requirements for an Effective Compliance and Ethics Program

Since 1991, the Guidelines have served as corporate America's blueprint in structuring effective programs to prevent and detect violations of law. Under the Guidelines, an organization that is convicted of a crime may be eligible for a reduced sentence if it had an 'effective' Program in place at the time the crime was committed. The Guidelines define the minimum requirements for an effective Program, which includes exercising due diligence to prevent and detect criminal conduct, as well as promoting an organizational culture that encourages ethical conduct. The Guidelines forward the following seven minimum requirements for encouraging ethical conduct and demonstrating a commitment to legal compliance:

1. The organization needs to establish standards and procedures (such as a code of conduct and appropriate policies and procedures) to prevent and detect criminal conduct.

2. The governing authority (i.e., board of directors) must be knowledgeable about the content and operation of the Program and exercise reasonable oversight with respect to its implementation and effectiveness. In addition, high-level individual(s) must be assigned overall responsibility for the Program and specific individual(s) must be delegated day-to-day operational responsibilities. Those with day-to-day responsibilities must report periodically to the high-level individual(s) and, as appropriate, to the governing authority on the effectiveness of the Program. To carry out these responsibilities, individuals must be given adequate resources, appropriate authority and direct access to the governing authority.

3. The organization must use reasonable efforts to avoid placing in a substantial authority position those whom the organization knew, or should have known through the exercise of

due diligence, had engaged in illegal activities or other conduct inconsistent with an effective Program.

4. The organization must take reasonable steps to communicate periodically and in a practical manner the Program's standards and procedures throughout the organization, including training that is tailored to members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and applicable agents of the organization.

5. The organization must take reasonable steps to:

    a. Ensure that the Program is followed, including monitoring and auditing to detect criminal conduct.
    b. Periodically evaluate the Program's effectiveness.
    c. Have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

6. The organization must promote and enforce the Program consistently throughout the organization through appropriate:

    a. Incentives to perform in accordance with the Program
    b. Disciplinary measures for those engaging in criminal conduct or failing to take reasonable steps to prevent or detect criminal conduct

7. After criminal conduct has been detected, the organization must take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's Program.

The Guidelines also call for the organization to periodically assess the risk of criminal conduct and take appropriate steps to design, implement, or modify requirements of the Program to reduce the risk of criminal conduct identified through the risk process.

Wide Applicability

The Guidelines apply to all organizations - public or privately held, large or small. It applies to virtually every type of organization, including; corporations, partnerships, associations, joint-stock companies, unions, trusts, pension funds, unincorporated organizations, governments and non-profit organizations. The Guidelines do not distinguish between organizational size, meaning all sizes and types of organizations are susceptible to the same Guidelines. However, the scalability to organizational size is an important theme as the Guidelines specify several times that 'reasonable' efforts are expected. Specifically, the Guidelines state "*the formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization*." Therefore, larger and more complex organizations are expected to have a more robust Program.

Integrating the Guideline's Minimum Requirements with the COSO Framework

Once an organization has a clear understanding of the minimum requirements for an effective Program, it is wise to sync-up the requirements to a control framework. In the U.S., the COSO Framework is by far the most popular control framework. The COSO Framework defines five

components (control environment, risk assessment, control activities, information and communication, and monitoring activities) and 17 supporting principles. All 'relevant' principles must be present and functioning to conclude that the associated component is present and functioning in support of concluding that objectives are effective. The COSO Framework views the 17 principles to be suitable for all entities except in rare industry, operating, or regulatory situations in which management has determined that a principle is not relevant to them. Refer to the COSO Framework's Executive Summary for an abstract of the framework, including the 5 components and identification of the 17 principles.

While it should be evident that all 5 components and 17 principles are relevant to an effective Program, here are some logical connections using the core of the seven minimum requirements as a basis:

1. **The organization needs to establish standards and procedures to prevent and detect criminal conduct.**

This one is synonymous with COSO Framework Principle 1, which is demonstrating a commitment to integrity and ethical values by setting a tone-at-the-top through the establishment of standards of conduct and evaluating adherence. Principle 1 is commonly considered the most important of the 17 principles since it is the bedrock of promoting organizational values and ethical expectations.

2. **The governing authority must be knowledgeable about the content and operation of the Program, and exercise reasonable oversight with respect to its implementation and effectiveness**.

This second minimum requirement is closely aligned with COSO Framework Principle 2, which is the board of directors demonstrating independence and exercising oversight of the development and performance of controls, including those established from Principle 1 above. This is a big one, perhaps only second in importance to COSO Framework Principle 1. Without independent board oversight of executive management, who is available to hold the CEO and other executives accountable? A recurring theme at most major U.S. frauds since 2000 (i.e., Enron, Worldcom, HealthSouth, Tyco, Adelphia Communications, etc.) is the lack of effective independent board oversight of management. The largest type of fraud in terms of dollars is financial statement reporting fraud and thus critical that effective oversight exists over the top executives to help prevent and detect this fraud.

3. **The organization must use reasonable efforts to avoid placing in a substantial authority position those whom the organization knew, or should have known through the exercise of due diligence, had engaged in illegal activities or other conduct inconsistent with an effective Program**.

Continuing with the matching to the COSO Framework, minimum requirement number 3 is addressed by Principle 3, which is the establishment of structures, reporting lines, and appropriate authorities and responsibilities. The key is ample due diligence through onboarding efforts and ongoing professional skepticism to help ensure that only ethical persons lead the organization.

4. **The organization shall take reasonable steps to communicate periodically and in a practical manner the Program's standards and procedures throughout the organization, including training that is tailored to members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and applicable agents of the organization**.

COSO Framework Principles 4 and 14 address minimum requirement 4. Principle 4 centers on competency enabled through training activities for all employees, agents and directors. Principle 14 addresses internal communications of objectives and responsibilities necessary for the proper functioning of controls, which are established through policies and procedures such as a code of conduct or conflict of interest policy.

5. **The organization shall take reasonable steps to ensure that the Program is followed, including monitoring and auditing to detect criminal conduct**.

Good governance practices and controls on paper means little if people and systems are not doing what they are supposed to do. Hence the importance of COSO Framework Principle 16 pertaining to ongoing and separate evaluations to ascertain if controls are properly designed and operating effectively. Monitoring activities assess whether controls outlined in the 5 COSO components and 17 principles are operating as intended. An independent internal audit function often does much of the heavy lifting on this front.

Another aspect of this minimum Guideline requirement is to have and publicize a system whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation. This is often accomplished through an ethics/fraud hotline, which relates to multiple COSO Framework Principles, including Principles 1, 14 and 15 when extended to external parties such as customers and vendors.

6. **The organization must promote and enforce the Program consistently throughout the organization through appropriate incentives and disciplinary measures**.

Incentives and disciplinary measures are a common topic of the COSO Framework, most notably in Principle 5 in holding individuals accountable and Principle 8 in considering the potential for fraud in assessing risks. People tend to perform as incentivized and the lack of appropriate disciplinary measures will send a powerful cultural message that people will likely get away with fraudulent behaviors.

7. **After criminal conduct has been detected, the organization must take reasonable steps to respond appropriately**.

This one is similar to Guideline requirement 6 in that it involves disciplinary actions, in this case after the fraud is detected. In addition to COSO Framework Principles 5 and 8, Principle 1 comes into play to address ethical deviations in a timely manner. In addition, Principle 9 pertains by assessing the impact of the criminal conduct in terms of control changes that should be considered to better prevent future frauds from occurring and perhaps identifying them in a more timely manner.

Evaluation of Programs

The Fraud Section of the U.S. Department of Justice's Criminal Division (Fraud Section) published a list of sample topics and questions entitled Evaluation of Corporate Compliance Programs in February 2017. It provides thought-provoking questions, including on risk assessment and risk-based training. This publication also includes questions on a wide variety of Program topics, including third-party management and M&A (merger and acquisition) integration. The publication is a must-read for insights on frequent questions the Fraud Section may ask in determining organizational culpability in the event your organization is a defendant in a federal court. Considering these question in conjunction with your Program and the COSO Framework is a worthwhile exercise.

Conclusions

While cultures will vary, healthy organizations must be proactive in developing and adhering to a Program that meets the Guidelines' seven minimum requirements. Leveraging the COSO Framework to a Program is not difficult and yet very useful in ensuring that the Program's effort ripples through the culture. Specifically, the components and underlying principles of control environment, risk assessment, control activities, information and communication, and monitoring activities are all critical to the ultimate success of a Program. Integration of Program requirements with the COSO Framework provides a strong basis for aligning objectives, risks and controls to best promote ethical behaviors.

Don't think of the COSO Framework solely as a regulatory tool to evaluate the effectiveness of internal control over financial reporting. Instead, think of it as a valuable framework for also addressing other reporting, compliance and operating objectives, including to prevent and detect fraud.

*****

Ron Kral is a member of Candela Solutions LLC, a public accounting firm with a national focus on governance, SEC compliance and internal auditing. He is an advisor, trainer and catalyst for companies to protect and grow client shareholder value. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. He is a facilitator of the *COSO Internal Control Certification Program* for the AICPA. Contact Ron at rkral@CandelaSolutions.com or www.linkedin.com/in/ronkral.

Candela Solutions LLC is a strategic CPA firm providing services to U.S. public companies that external auditors cannot due to independence concerns. Visit us at www.CandelaSolutions.com.

This is an article from the Governance Issues™ Newsletter, Volume 2017, Number 2, published on August 4, 2017.