Merging Two Compliance Universes

Compliance and Ethics

For over 25 years, the in-house community has modeled corporate compliance programs on Federal Sentencing Guildines (FSG) — which outline seven elements for effective ethics and compliance. There have been, and will continue to be, many advantages to operating under these guidelines. The FSG comprise common sense principles of sound governance aimed at effectively managing compliance and ethics risks. Moreover, when companies discover and report that one or more of their employees has violated the law, US courts and the US Department of Justice provide significant penalty reductions to companies that can demonstrate that their compliance programs satisfy the FSG requirements.

For more than 24 years, a separate internal control and enterprise risk management framework was evolving and has been widely adopted by both companies and regulators. In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the Internal Control – Integrated Framework (the Internal Control Framework) to help businesses and other entities assess and enhance their internal control systems. COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for regulators such as the US Securities and Exchange Commission, and for educational institutions.

In 2001, COSO initiated a project to develop a framework that would be readily usable by management executives to evaluate and improve their organizations' enterprise risk management.

This work culminated in the publication in 2004 of the *Enterprise Risk Management — Integrated Framework* (the ERM Framework). This document expands on the Internal Control Framework, providing a more robust and extensive focus on the broader subject of enterprise risk management.

In 2013, COSO published an update to the Internal Control Framework detailing the following 17 principles of internal controls:

Control environment

1. Demonstrates commitment to integrity and ethical values;
2. Exercises oversight responsibility;
3. Establishes structure, authority, and responsibility;
4. Demonstrates commitment to competence;
5. Enforces accountability;

Risk assessment

6. Specifies suitable objectives;
7. Identifies and analyzes risk;
8. Assesses fraud risk;
9. Identifies and analyzes significant change;

Control activities

10. Selects and develops control activities;
11. Selects and develops general controls over technology;
12. Deploys through policies and procedures;

Information and communication

13. Uses relevant information;
14. Communicates internally;
15. Communicates externally;

Monitoring

16. Conducts ongoing and/or separate evaluations; and,
17. Evaluates and communicates deficiencies.

There are many parallels between the Integrated Control Framework, the ERM Framework (the COSO frameworks), and the FSG. But, unlike the FSG, which focuses exclusively on compliance and ethics risks, the COSO frameworks provide guidance on managing all four aspects of enterprise risk: strategic, operational, reporting, and compliance. In addition, the COSO frameworks have a heavy emphasis on accounting controls and ensuring accurate financial reports. Nevertheless, compliance and ethics professionals might maximize the effectiveness of their compliance and ethics programs by bringing the COSO and FSG universes together. Specifically, doing so may afford you the following benefits.

Reducing fraud risks

In well-run companies, armies of accountants are responsible for managing financial reporting fraud risks. Although your accountants can and should design and implement internal financial controls, it's important to remember that many compliance departments — including, perhaps, your own — were created in response to financial reporting fraud that occurred under company financial professionals. Despite improved controls, fraud remains near the top of every corporation's list of compliance risks. Because your accounting colleagues rely on the COSO frameworks to manage fraud risks, it is imperative to understand the COSO frameworks and work with your accounting colleagues to determine how you can contribute to the cause.

Effective tools

The FSG set forth the elements of an effective compliance program, but provide little guidance on how you might actually get it done. Conversely, the COSO frameworks provide extensive practice guidance. For example, the ERM Framework has a companion "Applications Technique" document that provides many pages of practical tips on how to implement an effective enterprise risk management program.

Impressing external auditors

If your compliance program is typical, it is subject to routine scrutiny by your external auditors. They may or may not be familiar with the FSG, but they are certainly familiar with the COSO frameworks because both they and their firms use them to measure the adequacy and effectiveness of internal controls. You can greatly increase the possibility of a positive outcome with your auditors if you take deliberate steps to align your compliance and ethics program with the COSO frameworks. In my experience, nothing makes an external auditor swoon more than when they hear a chief compliance officer use COSO terms like "control environment."

Presentations to senior management and the board

Despite the fact that compliance and ethics programs have been around for decades now, it is still a relatively new function in many companies. As a consequence, many corporate executives and directors are not particularly clear about what a compliance department does and how its work fits into the company's broader enterprise risk management efforts. Fewer are familiar with the FSG. However, many corporate executives and directors are familiar with the COSO frameworks. Therefore, you can use the COSO frameworks to help your management team understand what the compliance and ethics function does by showing them how it fits into the broader enterprise risk management scheme.

Collaboration

Managing compliance and ethical risk in a corporation is a team sport. To be effective, compliance and ethics professionals must collaborate with many other corporate functions to get the job done. The COSO frameworks provide a uniform point of reference that can be relied upon to define roles and coordinate efforts. In doing so, you might use some of these tools to collaborate with your controllers, finance professionals, and internal audit teams to engage in a joint exercise to identify and remedy key control weaknesses.

So, instead of flying solo, bring the FSG and COSO frameworks together to maximize your

effectiveness and help your firm better manage its compliance and ethics risks.

Jim Nortz

Founder & President

Axiom Compliance & Ethics Solutions, LLC