CEP Magazine - February 2021
Aligning risk and compliance

By Gerry Zack

Please feel free to contact me anytime to share your thoughts: +1 612.357.1544 (cell), +1 952.567.6215 (direct), gerry.zack@corporatecompliance.org.

- twitter.com/gerry_zack
- linkedin.com/in/gerryzack

As I write this in late November, we are only two weeks removed from the publication of *Compliance Risk Management: Applying the COSO ERM Framework* by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). SCCE & HCCA authored this publication for COSO, and it represents the first comprehensive guidance aimed at aligning two widely used frameworks: the compliance and ethics program model from the United States Sentencing Commission that is the foundation for our profession and the enterprise risk management (ERM) framework published by COSO. The COSO framework is one of two frameworks commonly used by risk professionals globally, with the other coming from the International Organization for Standardization.

So why is this guidance necessary, and how does it benefit the two professions? In some organizations, there is already a strong dialogue between risk and compliance professionals, perhaps even being side by side in the same department. But in many organizations, the risk and compliance functions are separate, and there are barriers between them. Different philosophies exist on how to manage compliance risk versus other risks. At a minimum, even if the core elements of how to approach risk are similar, different terminology is often used.

But regardless of whether separate or combined into a single department, each profession can learn from the other. And this publication aims to align the techniques and characteristics of both fields, resulting in a powerful tool that combines the best of both worlds.

A quick pair of examples might help to illustrate what I mean, but please understand that they are by no means intended to imply any broad conclusions about either profession; they are merely recent real-life experiences that support my point. Some risk professionals focus very heavily on the risk assessment aspect of risk management and attempt to quantify and measure everything, an approach that works well for something like managing interest rate fluctuations. But compliance risk management benefits from also considering culture, training, communications, and other factors that are harder to apply strict formulas to.

But one thing that the COSO ERM framework appropriately focuses on is the connection between risk management and strategy, especially as it relates to creating and preserving organizational value. Compliance and ethics professionals sometimes fail at touting the value that an effective compliance and ethics program brings. We sometimes allow ourselves to be painted as a "cost center" rather than a creator and preserver of value.