

COSO Proposes Update to Enterprise Risk Management Framework

Changes to the risk management framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) are underway. COSO recently released an exposure draft that updates its 2004 integrated enterprise risk management (ERM) framework.

Following COSO's enterprise risk management framework is not required, but organizations often model their processes and systems after it because COSO principles are widely considered the gold standard in managing risks. Even organizations that have not used COSO's risk management structure as a guide in the past should review the proposed changes closely, as they may indicate how ERM best practices are evolving.

What's Changing in COSO's ERM Framework?

Enterprise Risk Management—Aligning Risk with Strategy and Performance, the exposure draft of the COSO changes, follows a format that is similar to COSO's Internal Control Integrated Framework in that there are core components and underlying principles. The five core components and 23 underlying principles simplify common ERM definitions, including risk events, uncertainty, severity, enterprise risk management, risk appetite and risk tolerance.

Risk's definition includes an emphasis on strategy and objectives. Organizations are encouraged to consider their core mission when selecting a risk strategy as well as considering how their approach to managing risks affects their risk profile and what obstacles they may encounter when trying to execute their approach. Appetite for risk and risk tolerance are also clarified, with risk tolerance being defined as the amount of risk an entity accepts at a certain performance level.

The proposed update also emphasizes how risk can have an impact on value. Whereas previous guidance emphasized ERM's role in minimizing risk, the updated

draft focuses on how ERM can be used to maintain value. The change comes so that ERM can be more of an active part in day-to-day organizational decision-making. Also encouraged is ERM's integration into culture.

Combined, the changes seek to make ERM more dynamic, so that an organization does not just set a strategy and let it play out, but constantly adjusts to address any change in performance.

Effect on Other COSO Guidance

The changes draw a line between ERM and internal controls. Organizations commonly use COSO's internal control framework, and there is some overlap between ERM and the control activities described in COSO's internal control publication. COSO makes clear in the exposure draft the ERM framework goes beyond control activities and that the ERM framework is designed to complement not override COSO's recommended internal controls framework.

The proposed changes are available on COSO's website. Comments are due to COSO by September 30, 2016.

If you have any questions or would like more information on the proposed changes, please contact:

Frank Campagna
CBIZ Risk & Advisory Services
RASinfo@cbiz.com | 866.956.1983



Our business is growing yours

Learn how CBIZ can help you identify ways to improve your Enterprise Risk Management at www.cbiz.com/ERM