U.S. GOVERNMENT ACCOUNTABILITY OFFICE
**441 G St. N.W.**
**Washington, DC 20548**

September 30, 2016

Mr. Robert B. Hirth Jr.
Chairman
Committee of Sponsoring Organizations of the Treadway Commission

**GAO's Responses to COSO's June 2016 Exposure Draft, *Enterprise Risk Management: Aligning Risk with Strategy and Performance***

Dear Mr. Hirth:

This letter provides the U.S. Government Accountability Office's (GAO) responses to the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Enterprise Risk Management: Aligning Risk with Strategy and Performance* exposure draft. GAO promulgates generally accepted government auditing standards and *Standards for Internal Control in the Federal Government* (Green Book) in the United States.

We support efforts to update the Enterprise Risk Management (ERM) framework to improve users' application of ERM's 23 principles. However, we believe there are areas of the ERM framework that can be improved, particularly for application to government entities.

We strongly believe that the ERM framework should provide clear guidance on integrating the framework and COSO's *Internal Control - Integrated Framework* to facilitate effective and efficient implementation of the two frameworks. This additional guidance could be issued as part of the ERM framework itself, as an appendix to the ERM framework, or as a separate guidance document. We are concerned that the lack of such clear guidance unnecessarily limits the usability of the framework and may result in inconsistent implementation.

The recently issued Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* requires, for the first time, federal agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the GPRA Modernization Act of 2010 and the internal control processes required by the Federal Managers' Financial Integrity Act of 1982 and GAO's Green Book. The Green Book adapts the principles in COSO's *Internal Control - Integrated Framework* for a government environment.

COSO's ERM framework acknowledges that "some aspects of internal control that are common to both this publication and *Internal Control—Integrated Framework* have not been repeated here (e.g., assessment of fraud risk relating to financial reporting objectives, control activities relating to compliance objectives, the need to conduct ongoing and separate evaluations relating to operations objectives)." It also notes that "other aspects of internal control are further developed in the Framework." However, the ERM framework does not clearly explain how a user would effectively and efficiently integrate the two frameworks. We believe that COSO is in the best position to develop such guidance.

We also believe that COSO should consider providing more guidance on applying the exposure draft to government entities. For example, COSO may consider the following:

- Providing further guidance for government entities in a separate document, thereby recognizing the unique government operating environment.

- Identifying unique considerations in a government entity's consideration of risk tolerance, such as natural or man-made disaster response.

- Clarifying how to incentivize government entity officials' management of risks, such as nonmonetary incentives.

In addition, the exposure draft's focus on entities with boards of directors makes it unclear how entities without boards of directors would implement some principles. For example, in principle 2, the section addressing authority and responsibilities includes entities with a single board of directors and a dual board of directors, but the section does not discuss other scenarios. COSO should consider using terminology, such as "stakeholders," that is more applicable to the government and nonprofit environment.

Further, the exposure draft indicates that ERM can be applied to a multitude of entities, including for-profit, nonprofit, and government entities, but it does not include many examples of how to apply the principles at entities that are nonprofit or governmental. COSO should consider using more examples, such as example 7.13 Sample Qualitative and Quantitative Measures, that show how to apply ERM at multiple types of entities, including nonprofit and governmental entities.

Lastly, the graphics that were introduced starting in chapter 5 of the exposure draft partially convey the message, but they could be improved to more clearly identify what each graphic is showing the user.

Thank you for this invitation to comment. If you have questions about this letter or wish to discuss any of our responses, please feel free to contact me at (202) 512-3133 or dalkinj@gao.gov.

Sincerely yours,

James R. Dalkin
Director
Financial Management and Assurance