GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 31, 2012

Mr. David L. Landsittel, Chair
The Committee of Sponsoring Organizations of the Treadway Commission

Subject: Committee of Sponsoring Organizations of the Treadway Commission (COSO) December 2011 Exposure Draft (ED) of an *Internal Control-Integrated Framework*

Dear Mr. David L. Landsittel,

This letter provides the U.S. Government Accountability Office's (GAO) comments on the exposure draft COSO *Internal Control – Integrated Framework* issued in December 2011.

GAO continues to support the COSO Integrated Framework and is in agreement with COSO that internal controls are an integral component that should be built into an organization's management and operations. GAO also supports the objective of using appropriate professional judgment with flexibility to find cost-effective ways of achieving strong controls.

The COSO draft guidance provides a good approach through the concept of principles and attributes of how to integrate various internal control components into a framework, assisting management and other interested parties in assessing the effectiveness of an entity's system of internal control and reporting.

Enclosure 1 details GAO's comments on the following areas where we believe the guidance can be improved, along with our specific recommendations:

Comment Summary:

- Clarify language used in classifying deficiencies and applicability of material weaknesses
- Improve general applicability of the COSO Framework to all entities
- Improve discussion related to information technology (IT)
- Improve discussion of outsourced service providers
- Emphasize safeguarding assets
- Improve consistency in presentation of attributes
- Clarify presentation of changes to the 1992 Version of Internal Control - Integrated Framework
- Clarify importance of management philosophy
- Need for completeness for reporting objectives in Executive Summary

Enclosure 2 contains our suggested language for changes to the discussion of information technology. Enclosure 3 contains answers to the specific questions on the website.

We thank you for considering our comments on this important proposed internal control framework as we work together on issues of mutual interest. Please contact myself on 202-512-3133 or dalkinj@gao.gov, or Heather Keister, Assistant Director on 202-512-2943 or keisterh@gao.gov, if you want to discuss any of our comments or need further information.

Sincerely yours,

James R. Dalkin
Director
Financial Management and Assurance

Enclosure 1

Clarify language used in classifying deficiencies and applicability of material weaknesses

We believe that terminology used for categorizing deficiencies in the design and/or operation of internal control should be consistent for all three types of control: operations, financial reporting, and compliance. Specifically, we believe the terms "material weakness" and "significant deficiency" should be used with respect to all three types of controls. Such terms are in common usage and, consequently, we believe that such terms convey the relative severity of control deficiencies. Using consistent terminology would also be clearer and less confusing in communicating deficiencies in internal control, particularly when all three types of controls are addressed. Further, we do not believe that "major/minor nonconformity" is an appropriate term because it is not commonly used with respect to the effectiveness of internal control, but rather is generally used in terms of compliance with laws and regulations.

The federal government has used consistent terminology to categorize all types of controls for many years and we believe that it has provided a consistent frame of reference for users to evaluate the significance of reported deficiencies in internal control. We recognize that using the terms "material weakness" and "significant deficiency" would require expanding the definition of the terms to address controls over operations and compliance, but believe that it could be readily accomplished. We believe that revised definitions should consider both the potential likelihood and magnitude of ineffective controls. We note that footnote 7 in the exposure draft provides a possible definition for a material weakness with respect to compliance controls.

Discussions related to preventive and detective controls should be consistent. We note that paragraph 292 discusses the two types of controls—preventive and detective—and that actions should be taken to correct detected unintended events or results. However, we also noted instances where the exposure draft used the terminology "prevent, detect, or correct." We believe that such terminology should instead be "prevent, or detect and correct" to be consistent with practice and paragraph 292.

Recommendation

We recommend that the term material weakness be used for classifying internal control deficiencies for all three categories of objectives. We recommend that the terms major and minor non-conformities be removed from the exposure draft.

We also recommend that COSO re-examine the exposure draft and wherever preventive and detective controls are mentioned clearly demarcate the difference by using the terminology "prevent, or detect and correct" as opposed to the current usage, "prevent, detect, or correct."

Improve general applicability of the COSO Framework to all entities

We believe that terminology should be sector neutral to reflect the broad range of users of the COSO Framework, including government, small businesses, and non-for-profit entities. For example, terms such as "board of directors" or "chief executive officer" may not be applicable to all users of the Framework and should be replaced by or appended with terms such as "those charged with governance" and "head of the organization," respectively. As another example, paragraph 103 states "Among the most significant benefits of effective internal control for many entities is the ability to meet certain criteria required to access capital markets, providing capital-driven innovation and economic growth." We agree that this is a benefit of effective internal control, but it is not necessarily a benefit for government and not-for-profit entities. Also, it would be helpful if there were more examples that are based on the government, small business, or not-for-profit sector. Consequently, while we noted that the Framework did contain some language to include government entity, small businesses, and non-for-profit organizations, we believe that the Framework should be reviewed and revised, as necessary, to be more sector neutral.

Another reason for sector neutrality in the COSO Framework is to enhance consistency with complementary internal control standards. GAO is responsible for issuing internal control standards for the federal government, and has issued *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1, November 1999). Our last revision to the standards in 1999 was based on the 1992 version of COSO's *Internal Control—Integrated Framework.* We believe that it is critically important to have consistent standards for internal control where appropriate, while recognizing that some differences may exist. We believe that many of the principles and characteristics described in COSO's Integrated Framework will be helpful for understanding and implementing internal control in government. Sector neutrality in the COSO Framework would contribute greatly to better consistency between the COSO Framework and GAO standards.

Recommendation

We recommend modifying the Framework to include terms that are applicable to all types of entities. We offer the following suggested language:

- Modify paragraph 9 on page 1 to read, "… and provide a board of directors,[1] **or those charged with governance,** with…"
- Modify footnote 1 on page 1 to read, "Hereinafter, the term "board of directors" refers to those charged with governance of an entity."

- Modify paragraph 121 on page 28 to read, "Individual behavior can be influenced by the knowledge that the chief executive officer**, (insert footnote here) or equivalent organizational leader,** has done the right thing…" The recommended language for the inserted footnote is as follows, "Hereinafter, the term "chief executive", or "chief executive officer" refers to the entity's organizational leader."
- Present the chapter titled *Roles and Responsibilities* on page 123 of the Framework as an appendix.
- Modify the examples contained in the Framework to include language that can be applied to an array of entities including government entities and not-for-profit organizations.
- Place the benefits relating to the ability to meet certain criteria to access capital markets located at paragraph 103, page 21, in the bulleted list under "Other benefits of effective internal control include:" in paragraph 104, on page 21.

Improve discussion related to information technology

Information systems have evolved significantly since COSO issued the 1992 Integrated Framework. We noted that the Framework did mention the changes in internal control system due to information systems. We believe it to be critical, however, that this new version reflect the risks posed by an organization's reliance on information systems and provide guidance on what types of control the entity should consider to mitigate those risks.

Framework does not adequately discuss factors that affect the nature and extent of risk associated with information technology

There are several factors that affect the nature and extent of risk associated with Information Technology (IT) controls for which the Framework does not contain a clear discussion. We believe that such factors would include:

- Nature of the hardware and software used;
- Configuration of the networks; and
- IT strategy.

For a definition of each of these items please refer to Enclosure 2.

Framework does not include guidance on the use of appropriate criteria for assessing the adequacy of information technology controls

In addition, we believe it is important that the COSO Framework guide the entity to develop an appropriate set of criteria for assessing IT controls. There are a number of examples of comprehensive criteria that have been published that can be used to

assess the adequacy of IT controls. For the federal government, criteria include GAO's "Federal Information System Controls Audit Manual" (FISCAM) and National Institute of Standards and Technology (NIST) information security guidance. Such criteria provide control objectives that should be achieved to have effective IT controls. Please refer to Enclosure 2 for examples of specific language regarding appropriate criteria for assessing the adequacy of information technology controls.

Framework does not adequately cover the objectives of confidentiality and availability of data

We concur with the three information processing objectives of completeness, accuracy, and validity. However, we believe that there are two additional objectives related to confidentiality and availability that are also relevant and should be included in the Framework. Controls over confidentiality are important to protect the confidentiality of personal information and to comply with various privacy and data breach laws, as well as to consider the potential risks or implications to an entity if personal information maintained by the entity is breached. Also, controls over availability are important to reasonably ensure that there is timely access to information. In the absence of controls related to availability, information and systems may be unavailable when needed. Weakness in controls related to confidentiality and availability can have a significant effect on an organization's ability to achieve its mission, as evidenced by publicly reported data breaches and website unavailability.

The Federal Information Security Management Act defines the terms as follows:

- confidentiality – reserving authorized access restrictions on information access and disclosure, including means for protecting personal privacy; and
- availability – ensuring timely and reliable access to and use of information.

In addition, the technology general controls in Principle 11 should include an appropriate discussion of controls related to contingency planning, which directly relates to availability.

Further, it seems that paragraph 311 should refer to the "completeness, accuracy and validity of technology processing," rather the "completeness, accuracy, and availability of technology processing."

Technology General Controls

We believe that the technology general controls in the Framework should be expanded to include security management controls. Security management controls provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. In our experience, such controls are critical to the effectiveness of technology controls and therefore should be separately presented. As discussed in GAO's *Federal Information System Controls Audit Manu*al, security

management controls provide reasonable assurance that security management is effective, including effective:

- security management program,
- periodic assessments and validation of risk,
- security control policies and procedures,
- security awareness training and other security-related personnel issues,
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
- remediation of information security weaknesses, and
- security over activities performed by external third parties.

Recommendation

We recommend a principle in the control activities component to contain a complete discussion of internal control over technology. The principle could read "The organization selects and develops controls over technology to support the achievement of objectives." We recommend this principle include the following:

- Factors that affect the nature and extent of IT controls, such as:
    - Nature of the hardware and software used
    - Configuration of the networks
    - IT strategy
- Guidance on the use of appropriate criteria for assessing the adequacy of IT controls, such as:
    - FISCAM
    - NIST Information Security Guidance
- Expanded discussion of general controls over technology related to the following control categories:
    - Security Management
    - Access Controls
    - Configuration Management
    - Segregation of Duties
    - Contingency Planning
    - Confidentiality
    - Availability

Improve discussion of outsourced service providers

We believe the impact of outsourced service providers on an entity's internal control system should be more clearly addressed in the Framework. While we noted discussion in both the control environment and monitoring sections of the exposure draft, we did not believe that this adequately addressed the topic. Since the 1992 Integrated Framework, entities have come to rely more and more on utilizing

outsourced service providers for critical functions of their operations. In particular, we believe that the Framework should specifically discuss the following issues in the monitoring section (paragraphs 392-393):

- Management's responsibility to obtain assurance over the operating effectiveness of internal controls of a service provider or have entity controls in place to mitigate the risk of using a service provider.
- Defining a process to review reports received from service providers to ensure the entity adequately addresses any identified risks to the internal control system.

Recommendation

We recommend that a separate paragraph be included in the monitoring section to clearly state the need for management to assume responsibility to obtain assurance over service provider's internal control as it pertains to the services being provided to the entity, including procedures such as a review of service provider reports or put in place effective controls to mitigate the risk of using a service provider. We also recommend that the exposure draft define a process to review the service provider reports and address any concerns that are raised.

Also we recommend that a discussion of outsourced service providers be included in the Control Activities component focused on user control considerations. We believe that the guidance found in SSAE 16[1] and ISAE 3402[2] provides a good framework for addressing service providers.

Emphasize safeguarding assets

The Framework should be revised to more clearly emphasize that safeguarding assets is related to all three categories of objectives for internal controls. We did note that the Framework suggests that safeguarding assets relates to the operations objectives of internal control. The Framework then discusses the safeguarding of assets as it relates to the reporting objectives. The Framework, however, does not clearly state in the discussion of the categories of internal control objectives that safeguarding assets is a subset of the three categories of internal control objectives.

Recommendations:

We recommend that the Framework clearly state in the discussion of the categories of internal control objectives that safeguarding assets is a subset of the three categories of internal control objectives. We suggest adding the following language:

---

[1] *Statement on Standards for Attestation Engagements 16: Reporting on Controls at a Service Organization*

[2] *International Standard on Assurance Engagement 3402: Assurance Reports on Controls at a Service Organization*

- Paragraph 23, page 3 - "A subset of these objectives is the safeguarding of assets. Internal Control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of an entity's assets."
- After Paragraph 46, page 9 - "A subset of these objectives is the safeguarding of assets. Internal Control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of an entity's assets."

Improve consistency in presentation of attributes

We believe COSO could improve the consistency of the presentation of attributes in the closing summary with the presentation of attributes in the preceding narrative. Each chapter that was a component of internal control contains a summary of principles and attributes located at the end which provides the user of the Framework with an overview of the component's principles and related attributes. The summaries can be found on pages 47-50, 71-74, 89-90, 104-105, and 116-117. However, the attributes located in the body of the Framework are not consistent with the attributes presented in the summary at the end of each chapter.

Recommendation:

We recommend modifying the attribute headings, contained in the body of the Framework, to be consistent with the attributes contained in the summaries on pages 47-50, 71-74, 89-90, 104-105, and 116-117.

Clarify presentation of changes to the 1992 Version of Internal Control - Integrated Framework

We believe COSO should expand Appendix B or add a new appendix that discusses the changes an entity that adheres to the 1992 Framework would need to make to remain in adherence with the 2012 version of the Framework. The exposure draft provides a summary of changes to the 1992 Version of the Internal Control - Integrated Framework in Appendix B on page 140. The summary describes broad changes made as well as changes made within the five components of internal control. However, the appendix does not summarize changes that the entity would have to make in order to adhere to the 2012 version.

Recommendations:

We recommend Appendix B be expanded, or a new appendix be added, to include a discussion of what changes an entity that adheres to the 1992 Framework would need to make to adhere to the 2012 version of the Framework.

Clarify importance of management philosophy

We believe that the discussion of tone at the top did not have a definitive statement linking the attitude and philosophy of management to having a profound effect on internal control. The Standards for Internal Control in the Federal Government states, "Management's philosophy and operating style also affect the environment. This factor determines the degree of risk the agency is willing to take and management's philosophy towards performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control."

Recommendations:

We recommend COSO include in paragraph 119 a statement similar to, "Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control."

Need for completeness for reporting objectives in Executive Summary

We are concerned that the reporting objectives, which focus on the reliability of reporting, do not appear to adequately address the need for information to be complete. Specifically, the term "reliability" may connote that the information presented is reliable, but not that the information is sufficiently complete so that a user would not be misled. This concept is different from the transaction-based concept that all items that should be included are included. It relates to whether the information is contextually complete. For example, fair presentation includes a concept that disclosures are sufficient to avoid misleading users. We believe that the reporting objective, which is discussed in several places, should be clarified by adding the concept of completeness or more clearly defining reliability to include completeness of the information reported.

Recommendations:

We recommend COSO include in paragraph 20 the phrase "reliability and completeness of information presentation."

Enclosure 2

Definitions of factors that affect the nature and extent of risk associated with IT controls:

- Nature of the hardware and software used - The nature of the hardware and software (e.g., type of processing, type of software development, dependency of financial reporting controls on IT, degree of centralization) can affect the nature and extent of IT risk.
- Configuration of the networks - The manner in which the entity's networks are configured can affect the related risks. For example, factors increasing risk include a significant number of internet access points that are not centrally controlled, networks that are not segmented to protect sensitive systems or information, or lack of technologies that enhance security.
- IT strategy - The consistency of the entity's enterprise architecture and IT strategy with its business strategies can affect the proper planning and implementation of IT systems and related security.

Discussion of appropriate criteria for assessing the adequacy of IT controls:

The nature and extent of IT control techniques needed to achieve the objectives of general and business process controls depends on the factors affecting IT risk. In a low risk environment, the controls generally need not be rigorous to meet the objectives. IT controls and objectives are summarized below:

General Controls

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. General controls include the following five general control categories:

- Security management, which provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;
- Access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;
- Configuration management, which prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended;
- Segregation of duties, which includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and
- Contingency planning, so that when unexpected events occur, critical operations continue without disruption or are promptly resumed, and critical and sensitive data are protected.

Business Process Application Level Controls

Business process application level controls, commonly referred to as "application level controls" or "application controls", are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing. The effectiveness of an entity's internal control system is dependent on the effectiveness of entitywide and system level general controls. Business process application level controls include the following four control categories:

- Application level general controls, or application security, which consists of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.
- Business process controls, which are the automated and/or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing. Specific control areas of business process controls include the following:
    - Transaction data input is accurate, complete, and valid.
    - Transaction data is accurately, completely processed by an application in a timely manner.
    - Transaction data output and distribution is adequately controlled.
    - Master data is adequately controlled (e.g., approval, review, and adequate support for changes to master data).
- Interface controls, which consist of those controls over:
    - accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and
    - complete and accurate migration of clean data during conversion.
- Data management system controls, which are relevant to most business process application because applications frequently utilize the features of a data management system to enter, store, retrieve or process information, including detailed, sensitive information such as financial transactions, customer names, and social security numbers. Data management systems include specialized data transport/communication software (often called middleware), data warehouse software, and data extraction/reporting software. Data management system controls enforce user authentication/authorization, availability of system privileges, data access privileges, application processing hosted within the data management system, and segregation of duties.

Enclosure 3

To assist you in developing your views of the *Internal Control — Integrated Framework*, COSO and PwC have prepared a series of questions for consideration. Respondents can answer these questions on the website. Those questions are reproduced here for reference as you consider the updated *Framework*.

General Questions

1. Are you a member of one or more of the COSO organizations? No
2. Are you responding on behalf of yourself or an organization or company? Government Accountability Office
3. Where do you reside? Washington, D.C.
4. Where within your organization do you apply the COSO *Framework*? Yes
   - Compliance activities
   - External financial reporting
   - External non-financial reporting
   - Internal management reporting (financial or non-financial)
   - Internal control reporting
   - Internal audit
   - Operations activities
   - Other
   - We do not use the *Framework* at this time

Overall Impressions on the *Framework* (answered on a scale of 1 to 5)

Answers below assume 5 is high and 1 is low

5. The updated *Framework* will help strengthen an entity's systems of internal control 3
6. The updated *Framework* is internally consistent and logical 4
7. The updated *Framework* is written in a manner that is understandable and provides ease of use 3
8. The updated *Framework* is applicable to organizations of varying legal structures and sizes, and operating in various geographies and industries 2
9. The updated *Framework* will impose additional burdens on entities' reporting on internal control—e.g., reporting on internal control over external financial reporting based on Sarbanes–Oxley Act of 2002 (SOX) requirements 2

9.a If you believe that there is an additional burden, is the change appropriate? If not, why not?
We believe the additional burden is appropriate

Questions on Specific Areas of Interest (answered on a scale of 1 to 5)

10. Compared to the 1992 framework, the updated *Framework* creates a higher threshold for attaining effectiveness of internal control 2
11. The 17 principles set out in the updated *Framework* are a complete set of principles 2

12. The 17 principles with related attributes are helpful in describing important considerations of an effective system of internal control 4

13. There are necessary changes to the principles 4

14. An entity can conclude that it has effective internal control if one or more of the 17 principles are not present and functioning 2

15. The updated *Framework* appropriately expands the reporting objective category (i.e. internal and external reporting, financial and non-financial reporting) 5

16. The expanded reporting objective, and the manner in which this objective category is presented in the *Framework*, does not diminish our ability to apply the *Framework* when reporting on internal control over external financial reporting 2

17. The updated *Framework* provides an appropriate balances of reporting, operations, and compliance related approaches and examples 3

Summary

18. Are there any other general comments that you would like to provide

Please refer to our comment letter for general comments on the exposure draft Integrated Framework.