G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 20, 2006

Dr. Larry E. Rittenberg, Chair
The Committee of Sponsoring Organizations of the Treadway Commission
University of Wisconsin, School of Business
975 University Avenue
Madison, Wisconsin 53706-1323

Subject: Draft *COSO Internal Control Integrated Framework – Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting*

Dear Dr. Rittenberg:

This letter provides the U.S. Government Accountability Office's (GAO) comments on the draft *COSO Internal Control-– Integrated Framework Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting* issued in October 2005.

As you know, GAO supports the COSO Integrated Framework and is an 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 flexibility with appropriate professional judgment to find cost-effective ways of achieving strong internal controls.

The COSO draft guidance provides good discussion of the unique characteristics of smaller companies and the challenges that smaller companies face in implementing effective internal control systems. GAO believes that the principles and attributes in the draft guidance are very helpful for illustrating how control objectives can be achieved. We also believe that much of the guidance will be useful to larger companies and other types of organizations as well. GAO applauds COSO for finding real examples that can be used for small businesses and for presenting an insightful and helpful discussion on small company perspectives.

At the same time, the draft guidance states that, in order for a company to have effective controls, it must accomplish each of the 26 principles, and that the related attributes for each principle are expected. We have concerns that such an approach to viewing the principles and attributes will cause companies and auditors to take a checklist approach and actions to meet the requirements in form rather than in substance. Such an approach may also be costly in terms of the levels of documentation created, and would in fact be contrary to the statements in the Executive Summary and Overview sections of the COSO guidance that call for consideration of risk, use of judgment, and consideration of the internal control system as a whole.

There are many different ways to accomplish effective internal control, depending on the facts and circumstances for each organization. We believe that the COSO guidance should emphasize the use of professional judgment and a risk-based approach that considers the company's individual circumstances when using the 26 principles and related attributes, rather than characterizing each of them as required and expected. Such an approach would not only help companies develop appropriate controls but also cost-effective controls. We believe that it is especially important to find ways for small business to develop internal controls at a reasonable cost.

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

- Emphasizing judgment and risk based approaches to applying the principles and attributes in the guidance.
- Including additional guidance about the purpose of controls and a risk based evaluation of their effectiveness.
- Incorporating a framework for information technology controls.
- Incorporating additional information and concepts in the guidance, including linking control activities to risk assessment, safeguarding of assets, the role of off-the-shelf commercial accounting software, disclosure controls, and concepts impacting account risk assessments.
- Clarifying the applicability of the COSO guidance to government entities.
- Clarifying presentation issues, including terminology, relationship of guidance to other COSO documents, and presentation of examples.

Enclosure 2 contains answers to the specific questions on your web site.

We thank you for considering our comments on these important proposed standards as we work together on issues of mutual interest. Please contact Jeanette Franzel, Director (202-512-9471 or franzelj@gao.gov), Abraham Akresh, Assistant Director (202-512-9361 or akresha@gao.gov), or me (202-512-2600 or steinhoffj@gao.gov) if you want to discuss any of our comments or need further information.

Sincerely yours,

Jeffrey C. Steinhoff
Managing Director
Financial Management and Assurance

Emphasizing judgment and risk based approaches to applying the principles and attributes in the guidance

We agree with many of the statements in the Executive Summary and Overview section that call for consideration of risk, use of judgment, and viewing internal control as a whole rather than as separate components. We also agree that smaller companies can and should use approaches to developing and implementing internal control that take into consideration their unique operating environments. (Indeed, this is true for all companies). However, we believe that there is significant risk that the COSO guidance, as drafted, will not achieve the above objective.

Both the Executive Summary and the Overview state that all 26 principles presented in the guidance should be in place for a business to achieve effective internal control over financial reporting. In addition, the guidance states that to have effective internal control, a company should implement a mechanism or methodology to accomplish each of the 26 principles. Supporting each principle are attributes that the COSO guidance describes as characteristics that are generally expected to be present within a company.

We disagree with the notion that every company needs to accomplish each of the 26 principles to have effective controls and that the attributes presented in the guidance are expected to be present within a company. We are concerned that the requirement for all 26 principles to be present will cause auditors and companies to resort to using a "checklist" approach rather than relying on professional judgment and risk-based approaches depending on the facts and circumstances of a company's situation. We view this requirement as contradictory to the statements in the Executive Summary and Overview that call for consideration of risk, use of judgment, and consideration of the internal control system as a whole. We believe that as drafted this will cause many companies to take measures to meet internal control requirements in form rather than in substance.

Recommendation:

We recommend that the principles in the guidance be described as characteristics and that the attributes be described as steps that management could take to meet a principle, in place of the current description of the principles as requirements and the attributes as expected characteristics. We offer the following suggested language:

"Supporting each element of the COSO framework are principles, which are characteristics that support each element. However, depending on unique factors in each company, it is possible to accomplish the goal of overall effective internal control over financial reporting without addressing each individual principle, particularly if compensating, complementary, or redundant controls are present. The objective is to demonstrate that effective internal control over financial reporting has been achieved. The use of judgment is critical in making these determinations. Management's objectives for establishing and maintaining effective internal control and the auditor's objective to determine whether such control is effective may

involve different judgments as to the nature, timing, and extent of procedures performed."

"Attributes represent steps that management can take to accomplish the principles, depending on the company's circumstances and characteristics."

Including additional guidance about the purpose of controls and a risk based evaluation of their effectiveness

Purpose of Controls

The guidance needs to clearly state the purpose and nature of controls over financial reporting. Controls over financial reporting are designed to provide management with an appropriate level of assurance that financial statements are not materially misstated, whether caused by error or fraud. The level of assurance is often referred to as "reasonable assurance," which represents a high level of assurance, but not absolute assurance. Individual controls are not expected to provide this assurance, but rather the total control system taken together needs to provide the appropriate level of assurance. For this reason, the guidance should emphasize the need to make judgments as to whether the company has sufficient and appropriate controls to provide reasonable assurance rather than a requirement for 26 principles and expected attributes.

Risk-Based Evaluation of the control system

We recommend that a risk-based approach for evaluating the control system be presented as part of the COSO guidance to assist management in making professional judgments about the effectiveness of control. It is based mostly on the audit risk model in the auditing literature. The overall risk of material misstatement is based on a combination of inherent and control risk. In evaluating risk of materially misstated financial statements, management should:

- Define materiality for the financial statements and the risk of loss of assets. Unless management has defined and reached agreement on what level of total misstatement or loss is acceptable, the process may be inefficient or ineffective.
- Determine the key balances, key assertions for each balance, the related control objectives, and whether those control objectives are adequately achieved.
- Define materiality for each balance and assertion based on facts and circumstances.
- Understand the inherent risks – if there were no controls, what could go wrong to cause misstatements; the inherent risks could be company wide or they could apply to specific accounts or specific assertions.
- Understand the controls, especially those that would prevent the inherent risks from causing misstatements or would detect them if they occurred; these controls may be company-wide (such as the control environment); or they may be for specific accounts or assertions.
- Consider the probability of a misstatement to the financial statements as a result of any problems detected.
- Determine whether the controls for each assertion are sufficient to prevent or detect and correct misstatements exceeding materiality for that assertion. If they are judged to be sufficient, the objective has been achieved (even though

controls might not be perfect). If not, find additional controls relating to that assertion or find a way to improve those controls.

Compensating, Complementary, or Redundant Controls

Compensating, complementary, and redundant controls are an important overall concept that should be explained in the Executive Summary and in other prominent places within the guidance. This concept is especially important to consider in smaller companies, which often use different approaches in achieving effective controls. Effective internal control can be achieved through various combinations of controls. The important question is, "Does the entity have an appropriate level of assurance based on all the controls combined?" A weakness in one principle or component could be compensated for by a control primarily designed to achieve a different principle or component. Management should evaluate the existence and effectiveness of all the controls together in forming an overall conclusion on internal control effectiveness.

The last sentence of the first full paragraph on page 6 that states, "The organization must consider whether the failure to achieve the principle results in a conclusion that the COSO component is not working and therefore is a significant deficiency." This statement implies that a significant deficiency in one component is indicative of an overall deficiency in internal control without respect to compensating controls. We suggest revising that sentence as follows: "The organization must consider whether <u>there are compensating, complementary, or redundant controls that mitigate the effect of the weaknesses in a particular COSO component to determine whether internal control over financial reporting is effective."</u>

Recommendations:

In order to provide additional guidance about evaluating controls and their effectiveness, we recommend that the "Overview" and "Smaller Companies Perspectives" sections of the guidance be expanded to include the following:

- A discussion on the purpose of internal control, and how management uses judgment to determine whether the company has effective internal control,

- A risk-based evaluation approach that uses professional judgment, and is based primarily on financial statement assertions and management assurance, and

- A discussion about the importance of compensating, complementary, and redundant controls, especially in the small company environment.

Incorporating a Framework for Information Technology (IT) Controls

The draft does not provide a framework for determining the adequacy of IT controls, including the determination of the risks associated with IT security. Without such a

framework, we are concerned that the IT examples in the guidance are not provided with adequate context and therefore could be misleading and perceived as a defacto standard.

We agree that there are several factors that affect the nature and extent of risk associated with IT controls. However, the draft would benefit from a clear discussion of such factors, which would be applicable to any entity. For example, we believe that such factors would include:

- **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 risks 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.

In addition, the COSO guidance should state that the entity should use 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 assessing 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, particularly "Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53)." Generally, such criteria provide control objectives that should be achieved to have effective IT controls. The nature and extent of IT control techniques needed to achieve these objectives depends on the nature and extent of the IT and other financial reporting risks. In a low risk environment, the controls generally need not be as rigorous to meet the objectives. While the organization of the different criteria varies, they generally include the same types of control objectives.

Such objectives generally can be summarized into the following broad categories:

- General controls
    - Security management
    - Access control
    - Configuration management
    - Segregation of duties
    - Contingency planning
- Application controls
    - Application security
    - Business process controls

        - Input
        - Processing
        - Output
        - Master Data
    - Application Interface and Conversion controls
    - Database controls

Recommendations:

To provide additional context and criteria for considering the adequacy of IT controls, we recommend that the COSO guidance be expanded to include the following:

- A high-level framework for evaluating risk associated with IT controls, and
- Guidance on the use of appropriate criteria for assessing the adequacy of IT controls.

The following tables provide additional details as example**s:**

Summary of Factors Affecting IT Risk	
Nature of the hardware and software used	The followings factors related to the nature of hardware and software used can affect the nature and extent of IT risk: o The type of processing (e.g., on-line, batch oriented, or distributed). o The nature and extent of access (e.g., internet or wireless access) o The type of software development (e.g., the extent to which the software is developed internally or customized versus vendor-supplied software; and the extent to which vendor-supplied software has have been thoroughly tested or undergone client processing to a degree that would encounter existing flaws.) o The nature and extent of identified weaknesses in the software. o The dependency of financial reporting controls on IT. For example, certain systems (e.g., ERP systems) may produce limited audit trails and/or have limited supporting information that can be used as a basis for applying certain types of controls. o The extent to which applications are decentralized. Highly decentralized applications, particularly web applications, increase information security risk by adding complexity to information security and potential vulnerabilities. o The extent of application of new or obsolete technologies. New technologies can increase the risk that secure configurations of such technologies may not be well developed or tested, or that IT personnel may not properly implement security over such new technologies. Obsolete technologies can increase risk because they may no longer be supported by the vendor and may include unpatchable vulnerabilities.
Configuration of the networks	The manner in which the entity's networks are configured can affect the related IT 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.

Summary of Information Technology Controls	
General controls	
Security management	1. Establish a security management program. 2. Periodically assess and validate risks. 3. Document security control policies and procedures. 4. Ensure that resource owners, system administrators, and users are aware of security policies. 5. Monitor the security program's effectiveness and make changes as needed. 6. Implement effective security-related personnel policies. 7. Ensure that activities performed by external third parties are adequately secure.
Access control	1. Adequately protect information system boundaries. 2. Implement effective identification and authentication mechanisms. 3. Implement effective authorization controls. 4. Adequately protect sensitive system resources. 5. Implement an effective access audit and monitoring capability. 6. Establish adequate physical security controls.
Configuration management (CM)	1. Develop and document CM policies, plans, and procedures. 2. Maintain current configuration identification information. 3. Properly authorize, test, approve, and track all configuration changes. 4. Routinely monitor the configuration. 5. Update systems in a timely manner to protect against known vulnerabilities. 6. Appropriately document and approve emergency changes to the configuration.
Segregation of duties	1. Segregate incompatible duties and establish related policies. 2. Control personnel activities through formal operating procedures, supervision, and review.
Contingency planning	1. Assess the criticality and sensitivity of computerized operations and identify supporting resources. 2. Take steps to prevent and minimize potential damage and interruption. 3. Develop and document a comprehensive contingency plan. 4. Periodically test the contingency plan and adjust it as appropriate.
Application controls	
Application security	1. Application security is properly managed (e.g., risks are assessed, appropriate policies and procedures are in place and users are aware of them, the effectiveness of application security is monitored, external processing is adequately secure). 2. Access to applications is adequately controlled (e.g., appropriate identification, authentication, authorization, audit and monitoring). 3. All changes to applications are properly controlled, consistent with the entity's configuration management processes. 4. User capabilities are appropriately segregated. 5. Appropriate contingency planning is implemented.
Business process controls	1. Data input into the application is accurate, complete, and valid 2. Data is accurately and completely processed by the application, in a timely manner. 3. Data output and distribution is adequately controlled. 4. Master data is adequately controlled (e.g., approval, review, and adequate support for changes to master data)
Application Interface and Conversion controls	1. Implement interface strategy (extraction, staging, data mapping/translation, import/migration) that defines how interfaces are to be deployed and managed on an ongoing basis. 2. Establish procedures for interface processing (ownership, method/tool,

	notification, timing, reconciliation, interruption and resumption). 3. Monitor Compliance with policies and procedures.
Database controls	1. Establish a database structure that supports the security environment. 2. Access paths to the database have been identified and controls implemented to prevent or detect access. 3. Implement authentication controls that limit access to the database based on users' business need. 4. Implement database auditing and monitor activities on a regular basis.

Incorporating additional information and concepts in the COSO Guidance

Additional Illustration and Description of the Link Between Control Activities and Risk Assessment

While the risk assessment section provides a fairly comprehensive example of an account risk analysis, including identification of relevant assertions, the control activities section (pp. 67-90) does not clearly show how control activities should be linked to such risks and assertions. While Appendix D provides a more detailed presentation of control activities by account, the control activities section should provide a more clear discussion and examples of how the entity should design controls in response to identified financial reporting objectives and related risks.

Second, Basic Principle Number 12 seems to overlap Basic Principle Number 13, and seems to be more process focused rather than control objective focused. COSO should consider clarifying the relationship between the two principles and whether Number 12 is consistent with the other basic principles.

The control activities section would benefit from more discussion of the logic behind establishing control activities in response to the risk assessment, and an illustration using specific accounts and assertion with the link between risk and control activities.

Safeguarding of assets

The guidance does not adequately discuss internal control over safeguarding of assets against unauthorized acquisition, use or disposition. Internal controls over safeguarding of assets may include controls relating to financial reporting and operations objectives. When determining the effectiveness of controls over financial reporting, consideration of safeguarding controls is generally limited to those relevant to the reliability of financial reporting. Safeguarding of assets is discussed in the control activities example on page 71 regarding board level policies for safeguarding of assets; however, there is no discussion of safeguarding as part of the risk assessment process. The 1994 amendments to COSO are important and should be discussed in the guidance for small public companies.

Role of Commercial Accounting Software (Packaged software)

The guidance (page 18-19) notes the benefits of packaged software with built in controls. However, the guidance needs to note that packaged software often allows the controls to be turned off and/or employees might not know what to do with the reports produced, so the reports may not be used to achieve effective control. In addition, the company culture may cause controls to be avoided; for example, by sharing passwords. The company should determine whether the controls in the software are understood and are actually being used as designed.

Controls over disclosures

The guidance should stress the importance of controls over disclosures in the financial statements. This is an area where small businesses often need to enhance their controls.

Additional Context and Guidance for Specific Risk Assessment

The following discussion and guidance should accompany the risk assessment matrix on page 61, as these are important concepts that need to be considered when using such a matrix:

- Role of double entry accounting – The guidance should recognize the importance of double entry accounting and the relationships among accounts in evaluating controls. For example, revenue and receivables are related; if there are effective controls over existence of receivables, the same controls are usually effective over occurrence of the related revenue, and the two sets of controls should be reviewed together. Other common relationships include inventory and cost of goods sold, and payables and expenses. This type of a cycle approach is an efficient way to review controls and should be explained in the guidance.
- The evaluation of controls needs to consider how accounts work, not just their balances. The balance sheet contains certain accounts that are merely sums of past transactions. For example, retained earnings may be a large material number, but it represents the sum of other numbers, and the process of properly preparing the financial statements will generally result in this balance being low risk, not high risk.

- Role of completeness for liabilities – Completeness is usually the key assertion for liabilities. In evaluating completeness risks, the company should not consider the recorded balance for liabilities, but should consider what could be missing. Taking percentages of accounts payable or accrued expenses to total assets is not appropriate if management is concerned with what might be missing. These examples should be replaced with real analytical procedures.

Recommendations:

We recommend incorporating the above concepts and guidance into the COSO guidance.

Applicability of the COSO guidance to government entities

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 were based on COSO's *Internal Control—Integrated Framework.*

The Office of Management and Budget (OMB) issues requirements for assessing and reporting on internal control in the federal government and has recently issued OMB Circular A-123, *Management's Responsibility for Internal Control* (December 21, 2004). The OMB requirements incorporate GAO's *Standards for Internal Control in the Federal Government.*

We believe that it is critically important to maximize our complementary agendas and 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 the COSO guidance document will be helpful for understanding and implementing internal control in government. GAO will consider the final COSO guidance in determining whether to modify or update the internal control standards for the federal government.

In the draft COSO guidance, we disagree with the statement that the 26 fundamental principles are equally applicable to government agencies (Executive Summary-- page 1). For example, many of the principles describe specific roles and responsibilities of Boards of Directors and Audit Committees. Usually, the governance structure of government entities would not include a board of directors or audit committee. Governments instead have other governance structures, such as appropriations and oversight committees at the federal level. Therefore, those principles would need to be adapted to be relevant in government entities.

Recommendation:

We recommend removing the reference to government entities in the executive summary (and elsewhere in the document).

Presentation Issues:

Terminology should be made consistent with Auditing Standards Terminology

The AICPA Auditing Standards Board will soon issue revised auditing standards dealing with risk assessment and related topics. These standards will change some of the terminology and concepts dealing with controls. We believe COSO should use the same terminology as the AICPA in order to avoid confusion (or at least reconcile the terminology used to the AICPA terminology). Some terms to use include "those charged with governance," "inherent risk," "control risk," "risk of material misstatement," and "compensating, complementary, or redundant controls." In addition, the AICPA has changed the 5 assertions in SAS 31 to 12 assertions; the assertions now include several devoted to disclosure. COSO should consider using the new assertions. As the AICPA standards are converging with the International Standards of Auditing, it is even more important to use consistent terminology.

Relationship to Enterprise Risk Management Guidance

The relationship of the new COSO guidance to the recently issued guidance on Enterprise Risk Management is unclear. The evaluation of controls for financial reporting should be part of the entity's risk assessment process, not a separate event.

Presentation of Examples

The examples in the guide can serve as a good source of ideas for management and others; however, there is a significant risk that they could become the de facto requirements for effective internal control or be taken out of context and misinterpreted by the way in which they are presented. We recommend that the examples be presented in an appendix or separate document. Many of these approaches and examples would be applicable or appropriate only when certain facts and circumstances exist.

Answers to specific questions on COSO web site

1. This document provides guidance that will help companies develop and implement internal controls over financial reporting.

   Response: Agree.

   We believe that the principles and attributes presented are helpful in developing and implementing internal control, but should not be characterized as required and expected.

2. This document will help smaller organizations strengthen their internal control processes in a more cost effective manner.

   Response: Not necessarily.

   As drafted, there is risk that companies and auditors will adopt a "checklist" approach that is not cost effective due to the principles being characterized as required and the attributes expected.

3. This document improves my/our understanding of the Internal Control - Integrated Framework.

   Response: Agree.

   The principles and attributes presented are helpful in developing and implementing internal control.

4. The 26 principles set out in the Guidance are sufficient for effective internal control over financial reporting.

   Response: Agree.

   However, The guidance does not provide a framework for evaluating controls, and we strongly disagree with requiring the 26 principles.

5. There are principles in the Guidance that are not required for effective internal control over financial control.

   Response: Strongly agree.

   Many of the principles are redundant and overlapping. There is a need to make it clear that not all principles are required, and the same attribute or principle might satisfy multiple control objectives or assertions.

6. This guidance will be useful to diverse groups, including management, internal auditors and external auditors

   Response: Not necessarily.

   We believe that the principles and attributes presented will be helpful to diverse groups for implementing and evaluating internal control, but not when presented as required and expected. Furthermore, the guidance does not provide a framework for evaluating controls.

7. Are there additional examples that you believe would enhance the guidance that you can provide?

   Response: Yes.

   As discussed in our comment letter, we believe that the guidance should be expanded to include discussion of the following:

   - the purpose of internal control,
   - a framework for information technology (IT) controls
   - how management uses judgment to determine whether the company has effective internal control,
   - a risk-based evaluation approach that uses professional judgment, and is based on financial statement assertions and management assurance,
   - the importance of compensating, complementary and redundant controls,
   - safeguarding of assets,
   - the role of packaged software,
   - disclosure controls, and
   - additional context and guidance impacting account risk assessments.

8. In helping plan for the future, are there areas where COSO can provide additional guidance?

Response: Yes. Given the significant changes in practice and the changes in the business environment since issuance of COSO's original Integrated Framework, it might be time to consider a future project to modify the original Framework. We believe the same framework should apply to all companies, regardless of size, with flexibility to tailor the approach based on risk and circumstances using professional judgment.