American Bankers Association
Building Success. Together.

Michael L. Gullette
Vice President – Accounting and Financial Management
202-663-4986
mgullette@aba.com

March 16, 2012

Board of Directors
Committee of Sponsoring Organizations of the Treadway Commission
Website submission: www.ic.coso.org

Re: Public Exposure Draft: Internal Control – Integrated Framework (COSO Framework)

Ladies and Gentlemen:

The American Bankers Association (ABA) appreciates the opportunity to comment on the Public Exposure Draft: Internal Control – Integrated Framework[1] ("the Draft"). ABA brings together banks of all sizes and charters into one association. ABA works to enhance the competitiveness of the nation's banking industry and strengthen America's economy and communities. Its members – the majority of which are banks with less than $125 million in assets – represent over 95 percent of the industry's $13.3 trillion in assets and employ over 2 million men and women.

Under the Sarbanes-Oxley Act of 2002 (SOX), publicly-held banking institutions are required to assess and (when applicable) obtain independent attestation as to the effectiveness of internal controls over financial reporting, using a framework such as the current one issued by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (the COSO Framework). In addition, all banks with over $1 billion in assets – public or private – are subject to a yearly attestation of the effectiveness of internal controls over financial reporting under the FDIC Improvement Act of 1991 (FDICIA). With the implementation of FDICIA, the banking industry was the first industry to be required to report on internal controls and use the COSO Framework.[2] With this in mind, we believe that changes to the COSO Framework will have a more significant impact on bankers than any other group of preparers.

Within the Draft, COSO primarily updates the original framework that was originally issued in 1992. The most significant change in the Draft is that COSO introduces seventeen principles, representing the fundamental concepts associated with the five integrated components of internal control from the original framework (control environment, risk assessment, control activities, information and communication, and monitoring activities). Supporting each of the principles are eighty-one attributes, representing characteristics associated with each principle. We understand that the principles and attributes are not meant to represent new thoughts or ideas related to the evaluation of internal controls, but they are intended to more explicitly codify and organize what COSO believes to be existing practice.

[1] December 2011Exposure Draft.

[2] While the regulations do not specifically require usage of the COSO Framework, they refer to COSO as a suitable and available framework. When the regulations were issued, COSO was the only framework developed in the US, thus, effectively requiring the COSO Framework.

ABA agrees that it is important to keep the COSO Framework relevant. We believe the Draft is written in a consistent and logical manner and, for companies that are new to the assessment or attestation process, it can greatly assist in the documentation and assessment of an entity's internal control system. However, we have two major concerns that need to be addressed prior to issuance of a final framework:

1. Due process must be reconsidered.
2. The level of detail should be reconsidered.

These points are described in more detail below.

Due Process Must be Reconsidered.

The COSO framework is one of the most widely-used internal control frameworks for the purpose of internal control assessment and attestation, both in the United States and world-wide. As a result, many consider the COSO Framework to be "the standard" for internal control assessment[3]. Given the importance that SOX and FDICIA internal control reviews have in the banking industry, as well as other industries, we believe these requirements to use the COSO Framework place due-process responsibilities on COSO that would be appropriate for a standard-setter.

We understand that COSO members may believe the organization is acting in a "thought leader" role, and not as a standard-setter. However, the wide general acceptance of the COSO Framework for SOX Section 404 assessments and attestations has virtually made the Framework *the* generally accepted internal control standard – effectively the required standard. As a result, we recommend that an open process be performed that helps ensure sufficient review of the Draft. Similar to procedures used by the Financial Accounting Foundation and the Financial Accounting Standards Board, such a process includes:

- Ensuring an open, transparent process, and
- Conducting outreach to key stakeholders both before and after issuance of exposure drafts to determine and anticipate stakeholder needs and interpretations of the Draft and to identify and reduce the likelihood of unintended consequences.

Unlike the FASB's process, in which stakeholders have the opportunity for significant involvement and observation during the development of a standard, to our knowledge, COSO has not operated under this type of process.

[3] While SOX does not refer specifically to the COSO Framework, subsequent documents by the SEC acknowledge the Framework's suitability as an internal control framework and that the vast majority of issuers use the COSO Framework in evaluating internal controls.

An important standard such as this needs to be carefully evaluated and discussed among stakeholders to ensure that the proposed framework is being interpreted in similar ways. With a three month comment period that has taken place during the busiest financial reporting time period for most companies, there has been insufficient time for stakeholder discussions to take place. As a result, it is difficult to address each of the eighteen Public Exposure Feedback Questions in sufficient depth. We note that regulators are members of the COSO Advisory Council, but only in an observer role. While we believe that COSO does not anticipate significant changes in usage and application of the Framework, we also believe that the proposed changes can open the door to undue external audit or regulatory expansion and documentation burdens. With this in mind, we believe the following questions (in addition to the concerns expressed above) must be addressed prior to issuance of a final Framework:

1. What analysis has been performed to determine that the proposed Framework in the Draft will continue to satisfy the criteria noted by the Securities and Exchange Commission (SEC) as a suitable internal control framework under SOX[4]?

2. Given that SOX 404 assessment and attestation relates to "financial reporting", will the SEC limit this legal requirement to *external* financial reporting, as defined in the Draft (as opposed to also including *internal* financial reporting)?

3. Since the COSO Framework (and that framework proposed in the Draft) is applicable not only for reporting, but also to the operations and compliance functions of an organization, will an entity be allowed to represent that the COSO Framework is utilized, even though it is used only for one of these aspects of internal control? Should the operations and compliance functions be segregated from the Framework?

4. The COSO Framework is generally applied by banking institutions solely to external financial and regulatory reporting[5]. Are there plans by banking regulators to require internal control documentation over operations (such as risk management) and compliance areas that conform to the COSO framework?

5. How will auditing organizations (including the Public Company Accounting Oversight Board) interpret the proposed 17 principles and 81 attributes to internal control? Will the principles and attributes become the necessary "checklist" that becomes the basis for auditors' and bank examiners' opinions related to, or documentation of testing on, internal controls?

[4] Per *SEC Release 33-8238* "Specifically, a suitable framework must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting."

[5] FDICIA requirements also require an assessment of an institution's compliance with laws and regulations pertaining to insider loans and dividend restrictions.

6. How do auditing organizations believe that the framework proposed in the draft should integrate the work and results achieved from other control frameworks, such as COBIT[6], as well as supplements issued by COSO[7]?

While some of these questions are pretty basic, our response to the Draft could change based on the answers obtained. For example, very little analysis has been performed to evaluate how the Framework in the Draft would impact analyses of controls over operations or compliance. We are unaware of significant efforts by banking organizations to integrate the COSO Framework into internal controls over those aspects of an organization.

The Level of Detail Should be Reconsidered.

Newly-introduced principles related to fraud, changes, and general controls over technology may cause confusion.

The main change proposed to the COSO Framework is the introduction of 17 principles, as well as 81 attributes that are applied to the existing five components of internal control. We generally believe that the 17 principles do a good job of helping set expectations and goal-setting for an organization. The principles provide a good basis for senior management, staff employees, and the Board of Directors to more effectively focus on and determine internal control priorities.

That said, we believe the overall level of detail presented in the Draft relating to both principles and attributes may provide too much detail, causing confusion in execution, assessment, and testing. For example, we agree that an organization should consider fraud in assessing risks to achieving the organization's objectives. We also agree that organizations should identify and assess changes that could significantly impact the system of internal control. However, as is noted in the Draft, these processes are normally performed within the organization's process to identify and assess all risks to the achievement of its objectives. We have a similar observation as to the principle relating to general control activities over technology and how it relates to the corresponding principle addressing all control activities.

We understand why the Draft proposes to list these principles separately. Their potential importance to a system of internal control should not be understated. However, listing them separately may add confusion in evaluating whether specific principles may be considered

[6] Control Objectives for Information and related Technology (COBIT) is developed by ISACA (formerly the Information Systems and Control Association).

[7] Paragraph 491 of the Draft insists that risk tolerance is not part of internal control, but is included in the Framework as a pre-condition to internal control. Therefore, this begs the question of whether auditors and examiners must determine whether a company's system addressing risk tolerance, a key concept in COSO's Enterprise Risk Management Framework, is effective.

COSO is also intending to issue a draft of a supplemental guide that focuses on internal controls over external financial reporting. ABA assumes that issuance of this draft will address concerns expressed to this overall Framework draft.

present and functioning when other principles are not, and how that impacts the achievement of the internal control objective.

Including attributes provides too much detail in the analysis.

ABA believes that the inclusion of the 81 attributes (which are primarily activities that address each of the principles) provides too much detail and will result in confusion as to how organizations should document and assess their internal control systems. We agree with others who have voiced the concern that the Framework proposed in the Draft could become a checklist for both companies and their auditors. The result will be unnecessary additional documentation for evidence that existing processes can be tracked to the proposed attributes. Unfortunately, the level of detail provided may also end up in less critical judgment applied to assess the overall system.

As we noted above, ABA believes that the COSO framework is the generally accepted internal control standard and, thus, each of these attributes, if approved, will become the "necessary hurdle to overcome" in order achieve an effective system of internal control. While we believe that the attributes represent activities that can be considered "best practices" at many organizations, not all these processes are necessarily explicitly performed at all organizations, and the amount of documentation required to overcome the hurdle will be excessive and often gratuitous. With this in mind, ABA recommends that the attributes be deleted from the final Framework. A less authoritative document, such as implementation guidance (or even merely an article written by an individual COSO member), could provide the attributes as a view of best practices.

Thank you for your attention to these matters and for considering our views. Please feel free to contact me (mgullette@aba.com; 202-663-4986) if you would like to discuss our views.

Sincerely,

Michael L. Gullette