The Institute of Internal Auditors

Dennis K. Beran, CIA, CCSA, CRMA, CPA, CFE
Chairman of the Board

Senior Vice President - Audit
JCPenney Company Inc.
6501 Legacy Drive
Plano, TX 75024 USA

Phone: +1-972-431-7112
Mobile: +1-214-244-4123
Fax: +1-972-531-7112
E-mail: dberan@jcpenney.com

March 31, 2012

Response e-mailed to www.ic.coso.org

RE: COSO Internal Control – Integrated Framework Public Exposure Feedback Questions, December 2011

Dear Sir/Madam:

The Institute of Internal Auditors (IIA), as the standards setting body for the international profession of internal auditing, has a passion for guiding organizations to achieve the highest standards of governance, risk management, and control – all designed for the sole purpose of fulfilling an organization's strategic objectives in the most efficient, effective, and sustainable manner possible. For those reasons, The IIA became an original member of the Committee of Sponsoring Organizations (COSO) and continues to this day to champion the governance principles that our COSO partners espouse.

The IIA's President and Chief Executive Officer serves on the COSO board and we have volunteer leaders serving on the Advisory Council and in other supporting capacities. Given the impact that the Internal Control – Integrated Framework (Framework) has had on governance, risk management, and control efforts coupled with the U.S. based Sarbanes-Oxley regulations which require U.S. public companies to align their controls to a generally accepted control framework, our Institutes' leaders have been resolute in offering our broad membership an opportunity to respond to the exposure draft in a more direct manner. As The IIA's Chairman of the Board, I am pleased to offer our membership's perspectives on the exposure draft.

We applaud the COSO team's efforts and transparency in sharing the basis for revisions, rationale behind the writing team's approach, and opportunity for submission of comments. Given the foundational nature of the Framework, as well as widely differing opinions on the style and nature of principles based documents, we want to acknowledge the difficulty that the writing team and Advisory Council have in balancing theoretical and practical objectives.

Our comments are based on discussions conducted by a core team of internal audit professionals who serve on The IIA's Professional Issues Committee (PIC). These professionals consist of Chartered Accountants, Certified Public Accountants, and Certified Internal Auditors who have worked in the public and private sectors, internal and external auditing, and small, medium, and large domestic and international companies. PIC is responsible for all exposure draft responses on governance, risk management, control, compliance, and auditing topics from regulatory and standard setting bodies around the world. In addition, PIC drafts the practice advisories and practice guides which are the basis for the implementation of the *International Standards for the Professional Practice of Internal Auditing (Standards)*. To ensure a broad representation from The IIA's membership, PIC members participated in forums in several cities across the U.S.,

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

solicited input from our membership and chief audit executives worldwide, as well as solicited and received input from The IIA's Institutes in other countries.

The following are our principal comments and observations. Detailed responses to the questions posed in the exposure document, and other matters related to the document, can be found in Attachment A.

1. The first concern is the decision not to further integrate strategic objectives and risk management into the Framework. Our team was concerned by the separation of broader enterprise risk concepts from internal control given that risk assessment is a fundamental necessity for control development. Controls mitigate risks, risk mitigation optimizes execution of operations objectives, and operations objectives achieve strategic objectives (strategic goals). We reference the following section in paragraph 69:

   "Setting the overall level of acceptable risk and associated risk appetite is part of strategic planning and enterprise risk management, not part of internal control. Similarly, setting risk tolerance levels in relation to specific objectives is not part of internal control."

   A lack of risk tolerance setting can limit an assessment of whether a control is appropriately designed to mitigate a risk. While the setting of risk tolerance is a management decision, the process and action of setting a risk tolerance is essential to the overall integrated Framework. The following principles speak to this alignment:

   - #6 - The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
   - #7 - The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
   - #10 - The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

   While some of our members would like the writing team to completely merge the COSO ERM concepts into this document, there are also members who believe that strategy setting and enterprise risk management should be kept as separate concepts given the maturity of ERM in many organizations.

   Our final consensus is that there is an opportunity for COSO to further integrate best practices for governance, risk management and control disciplines while remaining risk-framework agnostic and without mandating additional requirements on organizations which may wish to focus solely on the objective of internal control over financial reporting. Such an approach balances the current need to refresh the Framework and allows organizations to utilize the Framework in the future in ways that the COSO board cannot anticipate today.

This approach is integral to establishing efficient and effective risk based controls tailored to the entity's needs. Such efforts increase the value of the refreshed Framework and facilitate integration with other existing risk and control practices, particularly for users outside the U.S. who are considering frameworks like ISO 31000 or Solvency II.

The refreshed Framework should:

- Speak fully to strategic objective setting and enterprise risk management, laying out how they are part of the overall organization governance framework.
- Clarify the degree to which strategic objective setting and enterprise risk management are inputs to the internal control Framework.
- Clarify the degree to which a lack of strategic objective setting and ERM efforts impacts the assessment of internal control.
- Clarify the degree to which an assessment of principle 6 which states, "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives" is dependent upon validation that such operational objectives as described are in alignment with strategic objectives. This may be addressed outside the Framework.
- Consider incorporating an updated graph (see Exhibit 3.10 in Attachment A) from the COSO ERM-Integrated Framework Application Techniques Manual as a reference to explain how the various components of strategy setting, risk management, and control apply. The COSO writing team should ensure that the recent paper on Risk Appetite and any changes to the Framework are appropriately reflected.

2. The second concern involves the principles and attributes in the document. IIA members clearly believe that principles based frameworks are a far better approach for tailoring the development and evaluation of internal controls to the specific objectives and circumstances of each organization.

   The principles and attributes in the draft were generally considered comprehensive and of value in the understanding of the components of internal control. The new draft emphasizes judgment in the evaluation of internal control effectiveness overall, as components are interrelated, yet it requires not only an overall evaluation of each component but additionally of each principle and attribute. This encourages management and auditors to think in silos within each element of the Framework versus taking a holistic approach to the evaluation of internal control over a given objective. This may encourage a checklist approach to assessing internal control rather than the use of judgment based on the significance of the objective, activity, or risk compared to the more relevant principles and controls that are working effectively versus a simple validation of existence of the principles and attributes outlined in the Framework. Paragraph 78 of the Framework states, "When a principle is deemed not to be present or functioning, an internal control deficiency exists." Internal auditing practitioners are concerned about the potential prescriptive nature of a process that results in a deficiency if any of the 17 principles are partially implemented or if any one principle is not in place in an entity's system of internal controls. Evaluating every principle for all key processes may not be necessary.

We believe that the Framework should guide the evaluator to ask whether the controls that are in place reduce the residual risk to an acceptable level and thereby provide reasonable assurance that the objectives under consideration will be achieved. Paragraph 81 covers this concept: "The term 'deficiency' refers to a shortcoming in some aspect of the system of internal control and has the potential to adversely affect the ability of the entity to achieve its objectives." The Framework should focus an evaluator's attention on understanding how an unmitigated risk can adversely affect an objective versus simply assessing whether a principle is in place.

We recommend the 81 attributes be clearly published in a manner that ensures they are not considered part of the Framework. We would further suggest that the term "attributes" be changed to "considerations" or another term which better reflects that the items are not an additional level of granular checklists which could be used solely to evaluate internal controls.

3. We support and applaud the expanded reporting objectives along with the operational and compliance objectives. However, the writing team should consider enhancing the Framework to more fully discuss operational and compliance objectives. Practitioners believe there should be a more balanced view of these objectives, as the draft focuses predominately on external financial reporting. Operational and compliance objectives should be addressed with similar depth, specificity and flexibility as the Framework allows on external financial reporting. At the same time, the Framework should clearly outline how it is the organization's decision to determine which objectives the entity wishes to address as part of its conformity with the Framework.

4. As discussed in item 2, the principles were considered favorably by members, although many do not believe the principles are evenly focused. We appreciate the writing team's need to blend theory and practical necessity. Fraud and IT general controls are among a number of considerations which bring risk to an objective. Reconsidering the level and definition of principles may be prudent so that they are consistent and applied across similar groups of objectives, risks, processes, systems, information, communication activities, environmental attributes and people factors. Fraud and IT may be more appropriately discussed as extensive attributes to other core principles.

5. We applaud the style, look and tone of the document which is clearly an appropriate refresh of the 1992 document. As the document nears final publication, we would suggest that a review for unnecessary wording and complexity be conducted. The revision has grown in length from the original 80 page document in order to enhance the direction to management and evaluators. Therefore, the writing team should ensure that the length is appropriate and writing succinct to support full adoption of the entire body of work.

   We believe it is imperative to clarify the difference between the Framework (pages 1-24) and other chapters (pages 25-139). Issuing the other chapters as a separate document could ensure a differentiation between the principles based document and additional optional guidance.

Thank you again for the opportunity to provide comments. We believe our members' comments and insights, once addressed, will ensure the Framework keeps pace with the substantial advances in governance, risk management and control processes inside and outside the U.S. ensuring that the fundamental COSO model stays relevant and embraced for the next 20 years.

The IIA welcomes the opportunity to discuss any and all of these recommendations with you. We offer our assistance to COSO in the continued development of this Framework and supporting guidance.

Best Regards,

Dennis K. Beran, CIA, CCSA, CRMA, CPA, CFE
Chairman of the Board

About The Institute of Internal Auditors
The IIA is the global voice, acknowledged leader, principal educator, and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing* (*Standards*). These principles-based standards are recognized globally and are available in 29 languages. The IIA represents more than 170,000 members across the globe and has 105 Institutes in 165 countries that serve members at the local level.

ATTACHMENT A

(Responses to COSO's Public Exposure Feedback Questions #1 through #18)

In answering these questions, there was uncertainty on whether the answers should be limited to the first 24 pages of the draft (the actual Framework per paragraph 68) or to the entire exposure draft. In general, our responses and ratings below are based upon review of the entire draft.

We intend to limit specific verbiage suggestions to the Framework (the first 24 pages of the draft). Additionally, we will refer to pages 1 – 24 as the Framework and pages 25 – 139 as guidance.

General Questions
1. **Are you a member of one or more of the COSO organizations?** Yes, the Institute of Internal Auditors is one of the original sponsoring organizations. The IIA is the global voice, acknowledged leader, principal educator, and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing* (*Standards*).
2. **Are you responding on behalf of yourself or an organization or company?** We are responding on behalf of our global organization. The IIA represents more than 170,000 members across the globe and has 105 Institutes in 165 countries that serve members at the local level.
3. **Where do you reside?** The IIA is based in Altamonte Springs, Florida, USA.
4. **Where within your organization do you apply the COSO *Framework*?** Not answered.

Overall Impressions on the *Framework* (answered on a scale of 1 to 5 with five being the highest or most in agreement)	**Summary Rating**
5. The updated Framework will help strengthen an entity's systems of internal control. The principles based framework is potentially a great improvement. The original conceptual framework clarified what internal control is, but did not give practical guidance on how to achieve it. Our members expressed concern, however, that it would not be applied as intended resulting in a checklist approach. The new draft emphasizes judgment in the evaluation of internal control effectiveness overall, as components are interrelated, yet it requires not only an overall evaluation of each component but additionally of each principle and attribute. This encourages management and auditors to think in silos within each element of the framework versus taking an holistic approach to the evaluation of internal control over a given objective. This will encourage a checklist approach to assessing internal control rather than the use of judgment based on the significance of the objective, activity, or risk compared to the more relevant principles and controls that are working effectively versus a simple validation of existence of the principles and attributes outlined in the framework. Of particular concern is the absolute nature of the statement in paragraph 78 which states, "When a principle is deemed not to be present or functioning, an internal control deficiency exists." Paragraph 81 states, "The term 'deficiency' refers to a shortcoming in some aspect of the system of internal control and has the potential to adversely affect the ability of the entity to achieve its objectives." The writing team should clarify how these statements should be applied when: • principles are partially working, and • some principles are working at a high state of maturity while others are non-existent. An example of these dynamics would be a fairly small, informally run organization with a strong commitment to integrity and ethics, a well-understood risk appetite, and unusually close oversight by the board, cascading down through the organization through management at all levels. Such	**3**

an organization may have little in the way of "specified…policies and procedures," but the well-understood culture and close supervision provides reasonable assurance that risks are managed and objectives achieved. The current Framework asks, "Are all 17 principles in place and functioning?" We believe the correct principle based question to ask is "Is the combination of governance, risk management, and internal controls in place to reduce the residual risk to a level acceptable by management (within legal, regulatory, and contractual expectations) and thereby providing reasonable assurance that management's stated objectives will be achieved?"	
6. The updated Framework is internally consistent and logical. There is logic in seeing strategy formulation and objective setting as pre-conditions of internal control. We feel, however, that it is inconsistent to exclude them because they should be well-controlled processes. If the right controls are not present within these processes, the resulting strategies and objectives are likely to be misaligned. The purpose of internal control is to support the achievement of the organization's strategic objectives in an ethical and compliant manner. COCO and Cadbury models include these activities as part of internal control and risk management systems.	**3**
7. **The updated *Framework* is written in a manner that is understandable and provides ease of use.** Most users of the original Framework felt it was hard to read and was written for accountants and auditors, not managers. Unfortunately, the new draft is likely to have the same effect. We present some of the issues and illustrative examples: • There are various tools that can be used to assess complexity of writing. One of these tools is the Gunning Fog Factor. We noted that the draft is written at a very high "fog factor." This will create barriers to comprehension, for both English and non-native English speaking readers. For example, paragraph 17 presents the very important concept of embedding controls in the process. Its Gunning Fog Factor is 21.68. According to the tool, this means that a reader would have to have 5.68 years of education after college graduation to comfortably read and comprehend the paragraph. A standard principle of business writing is that no piece of writing should have a fog factor above 12. • Sometimes, the use of words is grammatically incorrect. For example, paragraph 118 states, "Establishing a strong culture considers, for example, how clearly and consistently ethical and behavioral standards are communicated and reinforced in practice." To "consider" is a thought process. The gerund "Establishing" cannot "consider." English speakers used to reading audit reports may not have a problem understanding this, but it is not correct. For business managers and non-native English speakers, this word choice is a barrier to comprehension. Examples of this type of "auditorese" abound in the draft. Rigorous editing is needed to make the entire document clear, concise, understandable and reader-friendly, especially for non-accountants, non-auditors, and non-native English speaking readers.	**2.5**
8. The updated Framework is <u>applicable</u> to organizations of varying legal structures and sizes and operating in various geographies and industries. • At the principles level, #2 and #3 regarding board of directors and board oversight may not be applicable to all the organizations referenced in the question. • At the guidance level, it is very U.S.-centric; organizations at lower internal control maturity levels will likely not meet the attributes. It will be burdensome for small companies if they have to try to prove compliance with every principle and attribute.	**3**
9. **The updated *Framework* will impose additional burdens on entities' reporting on**	**3.2**

internal control—e.g., reporting on internal control over external financial reporting based on Sarbanes–Oxley Act of 2002 (SOX) requirements. • The amount of additional compliance burden is dependent upon the expectation of the SEC, the PCAOB, and external auditors. • At the principle level, they are similar to the 1992 Framework. At the guidance level, there are now 81 attributes. Now that companies have stabilized their SOX programs, there is a concern that demonstrating compliance with the updated Framework will require changing the SOX processes and create non value-added work. • At a minimum, companies will be compelled to map their components, principles, and attributes to their SOX Programs and then, identify and remediate any gaps. Companies with a centralized SOX program will require fewer resources to complete this update. Considerable resources are required in a decentralized environment if each process owner (a company may have hundreds) has to conclude for each component, all 17 principles and each attribute. • There is a concern that the absence of, or partial implementation of, a principle will result in a "deficiency" or "significant deficiency" that would prevent the company from concluding their system of internal controls is effective. We believe this is not indicative of a principle based approach.	
9a) If you believe that there is an additional burden, is the change appropriate? If not, why not? The principles and attributes approach, if used as intended, could lead to a more meaningful evaluation and definitively provide management and evaluators with more guidance on the potential design and considerations for internal control. At the same time, it is very likely that the evaluation will turn into a checklist exercise. Supporting attributes, as noted previously, are good but must be viewed only as considerations that may or may not be needed to conclude that internal controls are sufficient. There is concern that many companies will have to re-map their controls to processes and risks. This concern is expressed most often by U.S. companies that believe they have an established, effective set of documentation to support their SOX reporting. There is a perception that the burden of moving to the updated Framework is not value-added as their existing controls for financial reporting have been deemed adequate by management and external auditors. The COSO board needs to consider whether we are refreshing the framework to assist the current process and expectations or are we raising expectations regarding what we mean by the "adequacy of internal control."	**2.7**
Specific Areas of Interest (answered on a scale of 1 to 5 with five being the highest or most in agreement)	**Summary Rating**
10. Compared to the 1992 framework, the updated Framework creates a higher threshold for attaining effectiveness of internal control. The Framework does not create a higher threshold, but more precise and specific requirements due to the 17 principles and related attributes. For instance, the component on risk assessment has additional guidance related to that component, but the overall threshold of what was expected under the 1992 Framework has not changed. As we noted earlier, care should be taken to ensure that the principles and attributes are not considered overly prescriptive and thus leaving less room for applying professional/management judgment. The specificity of the principles and attributes make it more difficult to say internal control is sound if critical aspects are missing or ineffective. Paragraphs 70 to 90 could be interpreted to require that existing systems be fully remapped and that management would need to conclude across numerous processes on all principles and attributes. If all principles are expected to be addressed substantially, this could create a higher threshold to support an effective assessment.	**3.5**
11. The 17 principles set out in the updated Framework are a complete set of principles.	**3**

Although considered fairly comprehensive in general, there are different ways to approach the principles (not necessarily by component). Both completeness and optimal mix are considerations. Below are some specific suggestions: • The principles do not sufficiently assess how the external environment may impact the risk profile and resulting internal control needs of the organization. • Principles speaking to accountability establishment, segregation of duties, adequacy of assurance process, priority setting, data governance, etc., are possible principles that cross components. Accordingly, assessment may be constrained by assignment of principles to specific components. The writing team may wish to consider how the principles are used to develop an overall evaluation of internal control versus black and white conclusions at the principle/component level. • Many have challenged the rationale to establish fraud and IT general controls as principles versus attributes. Listing them as principles runs contrary to the theory of the framework concept which requires the document to not identify the specific risks but ensure appropriate risk assessment. At the same time, we realize the practical focus that all organizations must have on fraud risk and IT risk in some area of their organization. As we have stated previously, being prescriptive on principles may drive assessments that are required by the objectives and risk profile of the organization.	
12. The 17 principles with related attributes are helpful in describing important considerations of an effective system of internal control. See responses to #5, 6 and 13.	**3.5**
13. There are necessary changes to the principles. Specific comments for change include: **<u>Principle 5</u>** Recommend changing to: "The organization establishes and holds individuals accountable for effective management of risk in the pursuit of objectives." Internal control is one of the risk management strategies. Risk can be mitigated, transferred, insured or accepted. Effective risk management includes the upside of taking advantage of opportunities and the downside of not preventing undesirable outcomes. Implicit in effective risk management is to be alert to new risks and changes in risk factors and levels as well as being held accountable for responding appropriately. **<u>Principle 6</u>** Recommend adding: "…the assessment of risks relating to achievement of objectives." (We believe this is the intent.) **<u>Principle 9</u>** Recommend changing to: "The organization identifies and assesses changes that could significantly impact the achievement of objectives." A change increases risk to objectives, good and bad, and requires reassessment of control applicability and design. **<u>Principle 11</u>** Recommend eliminating this principle. IT general control activities do not need to be separated from control activities. They are control activities and should be assessed in combination with all controls relied upon for the achievement of objectives just like other process risks. **<u>Principle 14</u>** Recommend changing to: "The organization internally communicates information, including objectives and responsibilities for effective risk management and internal control…"	**4.3**

Recognize internal control as a response to effective risk management. Consider describing how communication processes disclose changes in risk appetite. **Principle 16** We recommend changing to: "The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning in an efficient and effective manner." Incorporate continuous improvement as one of the objectives of the evaluation. **Principle 17** Recommend changing to: "The organization evaluates and communicates internal control deficiencies and improvement opportunities in a timely manner…" This supports the objective of continuous improvement, not just correcting problems and errors.	
14. An entity can conclude that it has effective internal control if one or more of the 17 principles are not present and functioning. All practitioners involved in our discussion believe there should be room for judgment in determining whether a control system is adequate for a given objective even if one or more principles are absent or only partially effective. • The updated Framework could be read as suggesting that an effective system of internal control is achieved if the principles and related guidance attributes for each of the components of the model are present and functioning. Judgment is necessary to reach that conclusion, not the completion of a "checklist" assessment of each principle. • Reasonable assurance requires, in most cases, a combination of controls across a range of COSO components. Controls are not necessarily needed for every principle. Effective controls for one component of the Framework may compensate for a lack of controls in another component. There should be room for judgment in determining whether a control system remains adequate if any given principles are only partially present by assessing compensating controls. • The Framework should be very specific and use examples to show that you can have errors due to internal control issues and still have an effective system of internal control. Considerations in making that assessment will include the frequency and number of errors, the significance of the errors, whether controls mitigated the effect of the errors within tolerances, the period of time during which errors occurred, and whether the risk of non-achievement of objectives remained acceptable. Judgment and relative compensating components or control environment elements could offset principle deficiencies.	**3.5**
15. The updated Framework appropriately expands the reporting objective category (i.e., internal and external reporting, financial and non-financial reporting). This change is welcomed by many and recognized as important by most people familiar with the COSO IC framework updates.	**4.2**
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. We concur.	**4.5**
17. The updated Framework provides an appropriate balance of reporting, operations, and compliance related approaches and examples. The IIA supports the expanded reporting objective to ensure it goes beyond financial reporting; however, COSO should enhance the Framework by expanding upon the discussion of operational and compliance objectives. Practitioners believe there should be a more balanced view of these objectives, as the draft focuses on external financial reporting. Operational and compliance objectives should be allowed similar depth, specificity and flexibility as the guidance allows for external financial reporting. This could be emphasized through the attribute guidance.	**2.7**

• In assessing overall effectiveness and related deficiency definitions for Compliance and Operations objectives, the example material appears to be too black and white. Assessing the adequacy of controls over operations and compliance may require more understanding of an organization's risk tolerance and expectations as well as significantly more judgment than an assessment over external financial reporting. Most companies have many of the issues illustrated and may not conclude that their system of internal controls is ineffective.	

18. Summary - Are there any other general comments that you would like to provide?
1. COSO should consider the addition of a reporting chapter or additional guidance in order to illustrate flexible alternatives for evaluating internal control systems for various stakeholders. Many stakeholders may not need a point in time conclusion on effectiveness of internal control. The COSO refresh needs to incorporate alternatives such as a maturity scale for reporting on internal control systems. Such an approach would be useful for organizations of different size and complexity.
2. On page 51 on the title page of the risk assessment section, the writers note that "Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives." The use of adversely in this sentence could imply that risk is only referring to negative events versus positive outcomes. The writers should ensure that the broader understanding of risk – threats, opportunities, and uncertainties – is understood. Such a broader definition is contained in nearly all contemporary risk management literature.
3. Consideration should be given to including a comment related to the effective date of the updated Framework to ensure that it replaces the existing Framework and there is no potential confusion about having two Frameworks existing at the same time.

Exhibit 3.10
Relating Mission, Objectives, Appetite, and Tolerance