executive report

ferf
financial executives
research foundation

sponsored by
RR DONNELLEY

IMPACT of the 2013 COSO FRAMEWORK

June 2014

Table of Contents

Executive Summary

The Committee of Sponsoring Organization of the Treadway Commission (COSO) included a precise summary of its objectives for the 2013 COSO Framework (2013 Framework) enhancement within the first page of the foreword to *Internal Control – Integrated Framework Executive Summary*:

> *"In the twenty years since the inception of the original framework, business and operating environments have changed dramatically. Becoming increasingly complex, technologically driven, and global, at the same time, stakeholders are more engaged, seeking greater transparency and accountability for the integrity of the systems of internal control that support business decisions and governance of the organization."*

As the 2013 Framework is not meant to be a re-write of the original framework (1992 Framework), it is an opportunity for organizations to refresh their existing internal controls as needed. This research report, sponsored by RR Donnelley, provides insights from professionals and thought-leaders in key roles in the early phases of the transition to the 2013 Framework. The report is intended to assist senior-level financial executives as they plan and execute their own transition in the months ahead.

We invited senior-level financial executives from various industries to offer their views on how the 2013 Framework will impact companies, where gaps between the two frameworks may appear, and what areas companies should focus on or are focusing on – notably including Outside Service Providers (OSP), Disclosure Management Solution (DMS)[1] and eXtensible Business Reporting Language (XBRL).

Methodology

FERF and sponsor, RR Donnelley, interviewed the following thought leaders:

- Charles E. Landes, COSO Board Member
- Charles E. Harris, Audit Partner at PwC LLP
- Jeff Getz and Sandra Herrygers, Audit Partners at Deloitte & Touche LLP
- Chris Jeffrey, Audit Partner at Baker Tilly
- Stephen McNally, Finance Director at Campbell Soup Company
- Keith Kawashima, Managing Director at Protiviti Inc.
- Director of Internal Controls at Fortune 500 Insurance Company
- Managing Director of Internal Controls at Fortune 500 Technology Company

[1] Disclosure Management solutions enable streamlining of financial statement assembly and review processes. For additional information please see ***Disclosure management: Streamlining the Last Mile,*** ***http://www.xbrl.org/sites/xbrl.org/files/resources/SAP%20Disclosure%20Managemenr%20paper%20v2a.pdf***

Summary of Interviews

We have summarized the responses of our interviewees below. However, we strongly suggest that you read the in-depth interviews in Appendix D, as well, for additional details and insights.

1. **Based on a poll by RGP[2] of more than 850 participants, 34 percent are familiar with the concepts of the 2013 Framework, but had not started implementation; and only 7 percent have completed the mapping process. Most companies contacted for interviews were in the initial stages of transitioning to the new framework**.

2. **The 2013 Framework was issued to "refresh" the 1992 Framework and make it easier to understand the components of an effective system of internal control.**

   Charles Landes, COSO Board member, shared that the objective of the Board with the enhancement of the framework was to "…freshen up the 1992 Framework…make clear what a company needs to do in order to have an effective system of internal control……easier to understand the components of an effective system of internal controls.." He also adds, "the principles were implicit in the old guidance and what we have done was to lift what was implicit to be explicit by calling it out in 'principles'."

   Chris Jeffrey, Partner at Baker Tilly, indicated that the 2013 Framework was a great improvement over the 1992 Framework. He states, "…the 1992 Framework was quite nebulous and left a lot to interpretation. While the new framework is still intended to be principles based, the addition of the seventeen principles with the points of focus underneath that, provide actionable steps that a company can take to implement their controls framework to get a better understanding…"

   Stephen McNally, Finance Director at Campbell Soup Company, stated that the enhancement "…encompassed key changes that have occurred in business over the past 20 years such as globalization, growing regulatory requirements, more complex business models, including the use of outside service providers in a much more significant way, greater reliance on technology, higher stakeholder expectations regarding the board and the board's oversight of risk management, identification of fraudulent activities, etc…."

[2]Resources Global Professionals (RGP) Webcast: Effective Transition to the 2013 COSO Framework on February 27, 2014.

3. **The new framework will not have a significant impact on organizations that already have a strong system of internal control.**

Landes comments, "If your current system of internal control is pretty strong and effective over the years and has been updated for built-in technology controls, I would think that moving from the 1992 Framework to the 2013 Framework would be relatively painless; however, if your current system of internal control isn't very good to begin with, you are going to have a lot more changes if you are trying to design and operate a system that would be in compliance with 2013 Framework."

Chuck Harris, Partner at PwC, agrees and states, "The impact of the 2013 Framework on a company will depend on how well the company understood and implemented the 1992 framework; that is, if management fully understood the principles implicit in the 1992 framework, there shouldn't be a significant impact in transitioning to the 2013 Framework."

4. **Companies agreed that there is minimal impact if strong controls were in place prior to transition; however, the most common gap is documenting existing processes.**

Keith Kawashima, Managing Director of Internal Audit Services at Protiviti, indicates that the biggest gap that his clients experienced is the need for additional documentation. He explains "...with the additional specificity that is contained in the new framework, clients had to update or add documentation to reflect or clarify controls, that in many instances, the company was already performing... for example, the added guidance around entity level controls may require more or greater clarification of the documentation of the related control activities."

A Fortune 500 insurance company director of internal audit shares "…We have a project plan in place to address any gaps which are solely documentation to reflect the points of focus that is within the 2013 Framework. The explicit points of focus were very helpful in understanding the intent of the controls."

The managing director of a Fortune 500 technology company shares the same experience, "…our mapping exercise of our existing SOX risks and controls to the seventeen principles identified very few gaps. The gaps were primarily documentation issues where we have existing controls but have not included them in our SOX design. These were primarily entity level controls."

5. **Auditors share that there is not one particular area that companies should focus their efforts on but should consider all five components.**

Harris indicates "…I think where companies, especially public companies, will spend most of their time on will be on the components of control environment, risk assessment, information and communication and monitoring activities. The reason is that companies have a fairly mature system around control activities because of Sarbanes Oxley (SOX) but perhaps less so with respect to these other components of internal control." He continues "…because those are the components that management is less familiar with, and the principles and the points of focus articulate important aspects of the controls that need to be in place for those principles to be present and functioning. Management's assessment may result in some "tweaking" of its system of internal control..."

Risk assessment is another important component, according to Jeff Getz and Sandra Herrygers, partners at Deloitte & Touche LLP, they indicate, "There is a new focus on the risk assessment component, which is key, because if your risk assessment is inadequate, then you likely have deficiencies in your controls. In particular, fraud risk assessment is called out as a separate principle in the new Framework, but wasn't as prominent in the 1992 Framework." Getz enforced the notion that companies cannot really spend enough time thinking about fraud.

6. **Companies should also consider controls related to: a) Information technology and b) OSPs which are a new focus in the 2013 Framework.**

a) Information Technology

Stephen McNally, Finance Director at Campbell Soup Company and member of the COSO advisory council, explains "…the new framework recognizes that technology is now a key part of controls going forward. Specifically, the 11th principle in the Control Activities component reads 'the organization selects and develops general controls over technology to support the achievement of objectives." Another perspective is how technology plays a role with the fifth component - Monitoring Activities, McNally explains, "During the COSO Advisory Council meetings, there was discussion around what monitoring looks like. Initially, it seemed that monitoring activities were heavily weighted to internal and external audits. However, technology allows us to do some real time monitoring through mechanisms like dash boards, comparing transaction details to predetermined thresholds for anomalies, monitoring trends and patterns that may raise red flags, and assessing performance via metrics..."

From the auditors' perspective, both Getz and Herrygers emphasize information technology (IT) as an area of focus in the 2013 Framework.. "The IT context in the 1992 Framework was light." Herrygers expands on this notion, "COBIT had a SOX for COBIT[3] guide whom many companies and auditors leveraged for IT concepts. The 2013 Framework embedded many of the same concepts. So even though there is additional content related to IT in the new COSO Framework, it may not be an area of significant change for companies that have already included those controls in their ICFR program."

b) Outside Service providers

COSO Board member Landes states, "The CFO needs to understand that even though a function is outsourced to a service organization, the company is still responsible for their system of internal control. Therefore, there has to be ways that they are monitoring the effectiveness of that service organization…" He explains that this may be difficult sometimes because this information may travel "…so quickly and at real time…"

Articulating this new focus on OSP, Getz notes, "Since the use of external service providers is more common today, COSO provided explicit content related to OSPs in 12 of the 17 principles. The underlying notion is that an entity's responsibility for controls extends to the activities performed on their behalf by OSPs. Therefore, a company should understand the OSP's activities and processes to be able to analyze the risks and help ensure that the appropriate controls are in place regarding those activities…" He adds, "Since a deficiency in an OSP's controls may be indicative of a deficiency in the company's controls, management should not depend solely on receiving a Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, (SSAE 16) report later in the year. Instead, companies should be proactively monitoring their OSPs throughout the year to make sure there are no surprises at the last minute. However, the extent of certain OSP monitoring depends on how significant the OSP's activities are to the company…" Herrygers expands on the use of OSPs, "There wasn't much content on OSPs in the 1992 Framework and some companies focused on getting service auditor's reports related to the control activities in place at the OSPs. Today, however, there is much more context in the 2013 Framework related to the other components—well beyond the control activity component to the OSP - some of these considerations may be satisfied through a service auditor report, but there are others that require more specific monitoring from the company."

[3] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Sarbanes-Oxley-2nd-Edition.aspx

Jeffrey also shares that the 2013 Framework may require more work around IT OSPs. He states "…there could be more work in and around outside IT service providers." For example, "…we were working for a client that outsourced an IT function and they chose to outsource to an IT service provider that did not have a SOC 1 report in place. We helped that company put mitigating controls in place that ultimately addressed the new COSO principles. However it wasn't a simple task. The framework is clear that companies need to do their due diligence around selecting an outside service provider and to make sure they select the right outside service providers that have appropriate controls in place, especially if the company needs to be SOX compliant. If an OSP does not have appropriate controls and cannot demonstrate the operation of those controls (such as in a SOC 1 report), I would recommend to my client not to use that OSP. "

7. **Depending on what function the Disclosure Management System (DMS) has in relation to the financial reporting will determine whether the auditor will consider it in their review of internal controls**.

Harris explains the concept of 'upstream and downstream' and how this concept will determine whether DMS will be in scope or out of scope of an audit. "Upstream implementations are those where DMS pulls information from the company's trial balance, ledgers and/or consolidation systems to generate the company's financial information to comply with regulatory requirements for external financial reporting, and will require the auditor to consider the controls around DMS, because the direct output now has a bearing on the audit... If that DMS is 'downstream', where the company does not use DMS to compile the required information to comply with regulatory financial reporting requirements, then the auditor has no responsibility to evaluate controls in connection with the audit. That is not to say that DMS or the information it produces is not important, or that management does not have an obligation to design and implement controls over the accuracy and completeness of the information input to or produced from DMS."

Furthermore, Kawashima explains that disclosure management solutions are an area where controls are needed, "… this is certainly an area where garbage in garbage out applies. If you don't have a control around the DMS to identify disclosure events and transition, no process in place to support those disclosures, and monitor what you are disclosing, a company runs the risk of doing it incorrectly. Whether under the old, or the new revised framework, a company must have a process in place to ensure that they are doing it right and are consistent."

8. **As XBRL is a form of reporting that companies should provide reasonable assurance as to its accuracy and correctness.**

Landes states that companies should consider internal controls around XBRL reports "…it is not a paper world anymore. It is therefore important to consider controls addressing where misstatements could electronically occur. For example, if the company has not done a very good job mapping the appropriate general ledger account to the XBRL code, when that is absorbed through XBRL by a user, there may be an error…"

Harris also shares the sentiments that controls around XBRL are important and explains the two aspects to XBRL. "The first is from management's standpoint, and I absolutely strongly believe that management should have controls around the XBRL reporting process and that those controls should be designed to ensure management's XBRL data is complete and accurate. The second aspect is from the auditor's standpoint. As of now, there is no regulatory requirement for the auditor to be involved in the tagging process or the reporting process for XBRL. Management may certainly engage the auditor, at its discretion, to test the accuracy of its interactive data as a project unrelated to the audit, but is not required to do so. Until that requirement changes, it is not going to be an audit driven event. Companies run a significant risk if management is not producing accurate XBRL information. For example, an analyst using inaccurate XBRL information may draw wrong conclusions about a company's financial position or results of operations. This, in turn, could damage a company's reputation, which in a competitive marketplace could have serious implications. This potential scenario once again underscores the importance of management implementing effective internal control over its interactive data process."

Kawashima explains "…if you didn't have the right controls in place in the last stage, and a defined process and supporting tools to allow for timely and accurate submission of the company's required information to the SEC for these various reports, a company can potentially put themselves at risk. There continues to be growing focus around controls that are in place over the submission of reports, including XBRL exhibits, to the SEC, or any other regulatory bodies for that matter. As the requests of these regulatory bodies are expanding, controls should expand as well."

9. **Both auditors and companies believe the new framework will provide ample benefits to improve current internal controls and provide far-reaching opportunities.**

Jeffrey feels, "For companies that already have a formal internal control framework in place, such as those companies that are already compliant with SOX, there will be some mapping; but if they

only consider this as a mapping or compliance exercise, they are missing an opportunity to take a look at their control environment to make some value-added changes based on the new framework. This new framework is very dynamic."

McNally agrees that there are benefits to the new framework. He explains, "…besides supporting management at public companies in meeting their SOX compliance requirements, the 2013 Framework can and should be leveraged throughout the organization, at the division, business unit, and/or functional level, to mitigate risk related to the achievement of operational, reporting and compliance objectives. The 2013 edition of COSO's framework can provide a common language regarding governance, risk management and internal control."

Another benefit, Kawashima shares is that the 2013 Framework will allow companies to "…have the opportunity to rationalize controls with the refresh, and highlight those that really matter. Also, they can now reduce controls that are not as important to organization to achieve…this is causing companies to review control by control and take a hard look at where they all fit in…"

From the corporate perspective, the director of a Fortune 500 insurance company expects the new framework to have future benefits of applicability beyond the SOX based compliance. For example, "..we want to use a similar approach to the framework in order to provide additional transparency to ourselves, regulators, senior leaders, etc. on how the system of internal controls work holistically, and giving the company a common language on internal controls."

The managing director of a Fortune 500 technology company notes that the framework was helpful all around. They stated "[T]the 2013 Framework has pushed us to evaluate our design against a deeper set of assumptions and requirements. It has reconfirmed our guiding principles to think broadly and deeply across the business to make sure we are considering all areas that impact the accuracy and completeness of our financial reporting and areas that present the risk of financial fraud within the business." The managing director adds that there are other benefits their organization experienced with the transition to the 2013 Framework. For example, "We have other areas of our business that operate compliance programs but leverage other frameworks (i.e., Five Elements of Compliance and Seven Essential Elements of Compliance.) The expansion of the 2013 Framework into the seventeen principles helps us better align our SOX system of internal controls with these other compliance frameworks. This increases our ability to quickly identify the common elements between our SOX program and these other compliance programs and enable these other programs to leverage our core design as the foundation for their design."

After transitioning to the 2013 Framework, the managing director believes, "The principles put more structure and define better what is meant underneath the different components. For example, the explanation of areas to consider under risk assessment will help companies think more broadly around potential risk areas like emerging markets, the impact of IT in their controls framework and fraud risk. The framework also requires a stronger linkage across areas. For instance, if there is an issue with an IT General Control, the company needs to clearly examine and document the potential impact to their control activities related to that IT area deficiency. For many companies who have been updating their risk assessments and controls design on a fairly rigorous basis over the past ten plus years, this will be more of a mapping exercise with some additional controls wrapped around the core design."

10. **PCAOB's Staff Audit Practice Alert No. 11 may provide insight into what companies need to focus on.**

Kawashima states "…what we see happening is the culmination of a few things; firstly, there has been ongoing scrutiny by the PCAOB of the work that external audit firms perform over the last couple of years. The PCAOB inspects some of the audits the firm completed, the conclusions that the firm came to, and the support for those conclusions and subsequently produces an inspection report, which highlight whether the work done by the external auditor supports and evidences conclusions made by the external auditor. Some of the common areas listed where evidence was deemed to be insufficient and would require external auditors to gather more data to support their conclusions were; reliance on work of others, management review controls, IT controls, etc. Then if you add to that the introduction of the revised COSO framework, it is easy to see that the efforts for most companies and their external auditors may continue to grow around the evaluation of internal controls over financial reporting."

The director of a Fortune 500 insurance firm notes that, "..In October 2013, the PCAOB issued the Staff Audit Practice Alert No. 11 - Considerations for Audits of Internal Control Over Reporting[4] (alert), provided some clear direction to all the public accounting firms of the PCAOB expectations around the auditing that is performed on certain control types. This alert included, for instance, IT controls, management review controls, etc. The alert is in line with the new COSO framework, but a bit more prescriptive because this is what they will be expecting of auditors, therefore, we are using as well to update our documentation."

[4] http://pcaobus.org/Standards/QandA/10-24-2013_SAPA_11.pdf

11. **Even though there will be changes in audit methodologies, the principles were already implicit in the internal controls that were implemented and tested in previous years.**

Landes believes that "…audit methodologies will not change a great deal, I don't expect audit fees will be much higher for an issuer in order to do an integrated audit. However, this assumes the issuer has maintained a good system of internal controls to begin with…audit costs should not be much more, because the principles are already implicit in what they auditor should have already been testing for."

12. **CFOs should put a cross functional team in place and make the transition a priority.**

Landes states "…Since the COSO framework starts with the tone at the top, CFOs, should assemble a cross-functional team to own the conversion. Also, the CFO needs to be serious about making this a priority and believe that the adoption of the new framework will result in a better system of internal controls which will ultimately reduce the risk of material misstatements. The lack of compliance may be embarrassing to a company's reputation and the company's ability to raise money in the capital markets. To me, it is an easy decision for a CFO."

Harris suggests, "CFOs should go ahead and make transition with two goals in mind. First, give new controls implemented upon transition enough time to operate so that management can conclude on effectiveness; and second, as I earlier indicated, make this transition before the auditors come in and conduct their initial testing. Remember, auditors cannot tell management what internal control framework to use – they can only audit the system of internal control that management has put in place."

13. **A good place to start the transition is to perform a gap assessment.**

Herrygers, Partner at Deloitte & Touche LLP, recommends that companies perform a 'gap assessment' by mapping their current controls to the 17 principles, and by considering the points of focus for each principle, to identify potential gaps. She further explains, "In some cases, the principles are more specific and prescriptive about what companies need to have in place to demonstrate that they have addressed a principle. We, at Deloitte, recommend companies focus their energies on the areas where there is new or enhanced content in the 2013 Framework."

Performing the gap assessment may help companies:

1) Identify the need to scope in other already existing controls; i.e., the company identifies a gap, but has other existing controls that were not assessed under the prior Framework;
2) Enhance existing controls, i.e., a company might have a control in place related to the principle, but it may not address all the specific attributes that are relevant and; thus, may need to be enhanced; and
3) Design and implement new controls to achieve the principle.

Jeffrey adds "…the real work will be for companies to look at their controls framework and understanding where the new principles are and making sure that they are covered. So the value of the new framework to a company comes in understanding where they have gaps, and conversely, understanding areas where they might be 'over controlled' and trying to reconfigure their control framework based on their assessment…"

14. **There are concerns that a company that has not adopted the framework by December 15, 2014, may receive a comment letter or questioning from the Securities and Exchange Commission (SEC), as to why it has chosen not to adopt the new framework.**

Although the SEC has not provided guidance as to if and when companies are required to transition to the new COSO framework, it has, however, hinted that it expects companies presently using the 1992 framework to transition soon to the 2013 Framework, considering that COSO has announced that the 1992 framework will be superseded as of December 15, 2014.[5]

[5] http://www.complianceweek.com/sec-drops-new-hint-update-to-new-coso-framework/article/320514/

Summary of Enhancements

The 2013 Framework did not change but strengthened and clarified the five fundamental components of the 1992 Framework - *Control Environment, Risk Assessment, Control Activates, Information & Communications and Monitoring Activities*. To accomplish this, COSO has articulated 17 underlying relevant "principles" to support the design, implementation and assessment of the five components.

To help organizations implement the framework, and achieve the goal of applying internal control, COSO has published the following documents:

1. *Executive Summary* – provides a high level overview.
2. *The Framework and Appendices* – provides the definition of internal control, describing requirements, components and principles for an effective system of internal control.
3. *Illustrative Tools for Assessing Effectiveness of a System of Internal Control* – provides templates and scenarios.
4. *Internal Controls Over External Financial Reporting: A Compendium of Approaches and Example*s – provides illustrations of how the enhancements can be applied in preparing external financial statements[6].

The new framework will help managements and boards of directors to:

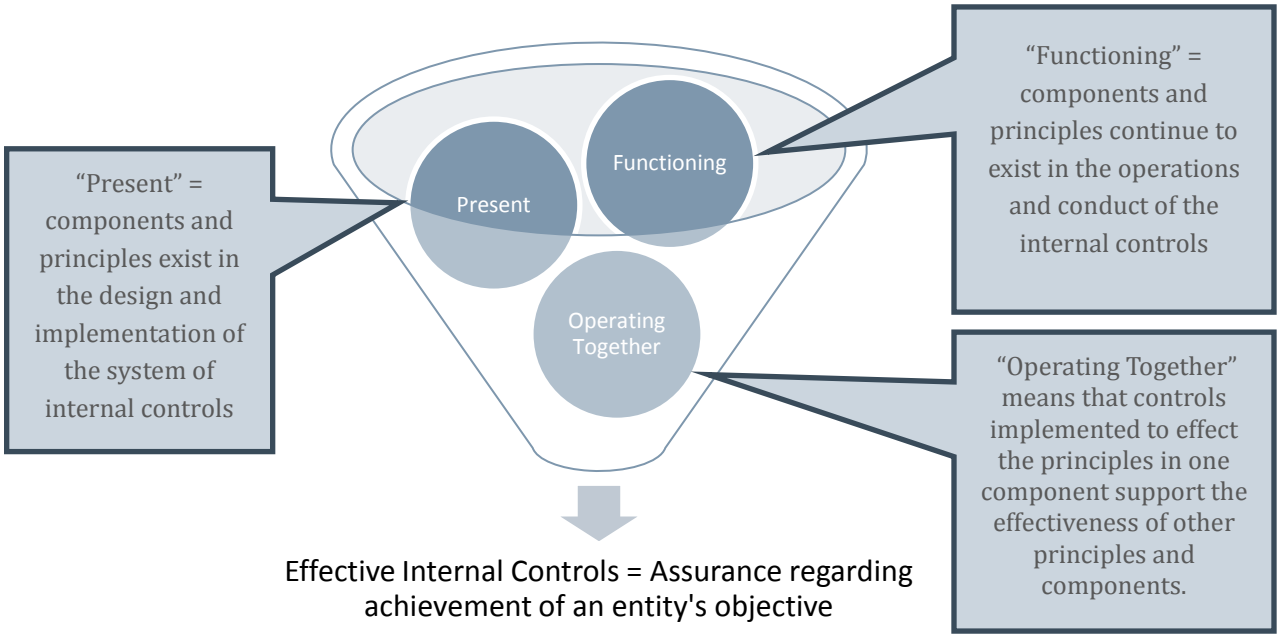
- Reconsider whether all of the five components and the relevant principles are present and functioning; and close any gaps;
- Enhance the risk management process through additional attention to fraud considerations and risks associated with outsourced processes;
- Consider expanding the application of the framework beyond financial reporting to other forms of reporting, operations, and compliance objectives; and
- Identify and eliminate inefficient and redundant controls.

If implemented effectively, the 2013 Framework should provide stakeholders a better understanding and obtain greater confidence in the effectiveness of internal controls.

[6]In addition, COSO also published the Enterprise Risk Management – Integrated Framework, which is intended to be applied in tandem to the Framework. As some concepts overlap, they are indented to be complementary.

To be effective, all the five components as well as the 17 principles supporting these components should be present and fully functioning. Additionally, the COSO board published "points of focus" which does not necessarily need to be present and functioning, but may help organizations to better understand the principles and design effective controls.

To reiterate, each of the five components and relevant principles must be present, functioning and operating together to achieve an effective system of internal controls.



To determine whether the components of the system of internal control are "operating together," management must aggregate the deficiencies across all components and make a determination of whether, in the aggregate, these deficiencies amount to a major weakness. If a major deficiency exists, even if management had concluded that each principle was present and functioning, the system of internal control could not be considered as effective.

To help get started, Appendix B provides the five components with their respective principles. [7]Appendix B contains selected illustrations from the COSO Compendium for how to select an OSP and IT security. Appendix C provides brief sample controls ideas for DMS and XBRL.

[7] Internal Control – Integrated Framework

Appendix A:

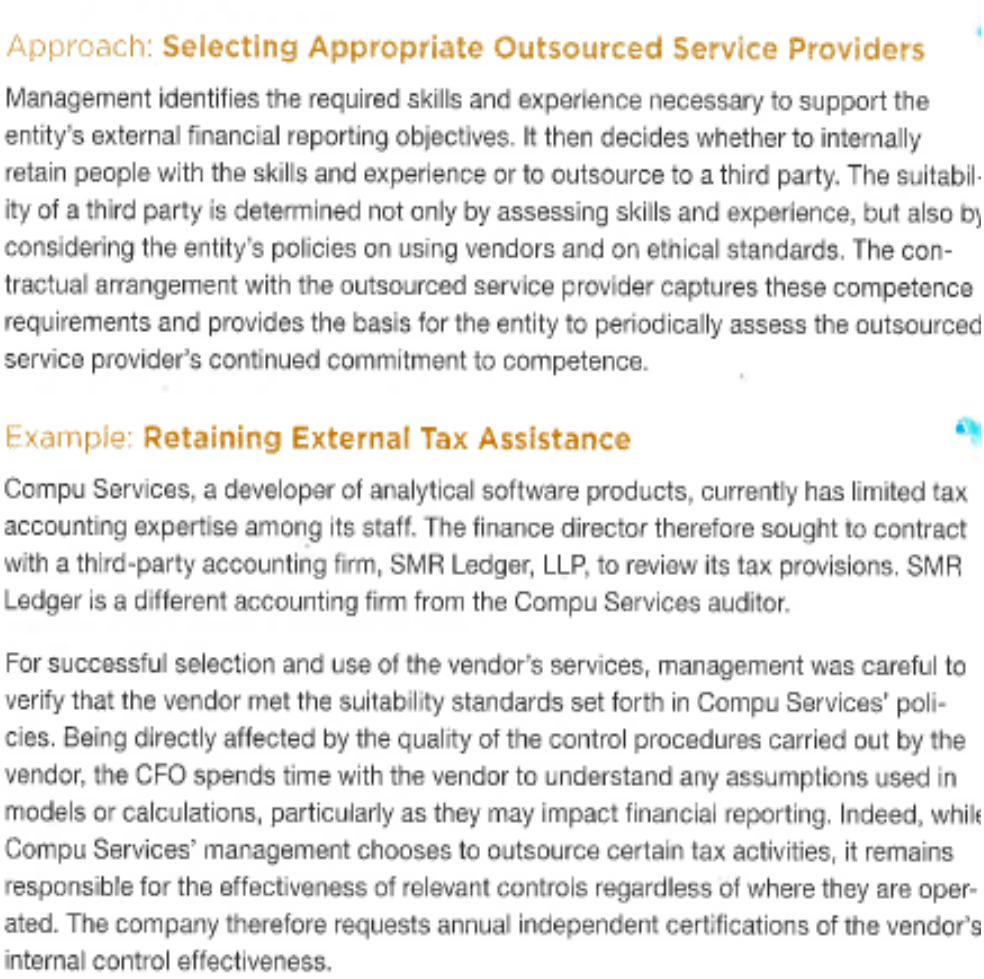
This chart illustrates the five core components from the old COSO framework that have carried over to the new. It also illustrates the 17 new explicit principles that COSO added to the new framework.

Component (NO change)	Principle (Explicit in 2013 Framework)
Control Environment	**1.** Demonstrates commitment to integrity and ethical values
	2. Exercises oversight responsibility
	3. Establishes structure, authority and responsibility
	4. Demonstrates commitment to competence
	5. Enforces accountability
Risk Assessment	**6.** Specifies relevant objectives
	7. Identifies and analyzes risk
	8. Assesses fraud risk
	9. Identifies and analyzes significant change
Control Activities	**10.** Selects and develops control activities
	11. Selects and develops general controls over technology
	12. Deploys through policies and procedures
Information & Communication	**13.** Uses relevant information
	14. Communicates internally
	15. Communicates externally
Monitoring Activities	**16.** Conducts ongoing and/or separate evaluations
	17. Evaluates and communicates deficiencies

Appendix B:

To help users apply the framework, *COSO's Internal Control over External Financial Reporting: A Compendium of Approaches and Examples (Compendium)* provides illustrations of how organizations may apply the principles set out in the 2013 Framework. Please note that the full Compendium can be purchased **http://www.coso.org/IC.htm**. We have provided examples:

- From page 39 **Selecting Outside Service Providers:**



Approach: **Selecting Appropriate Outsourced Service Providers**

Management identifies the required skills and experience necessary to support the entity's external financial reporting objectives. It then decides whether to internally retain people with the skills and experience or to outsource to a third party. The suitability of a third party is determined not only by assessing skills and experience, but also by considering the entity's policies on using vendors and on ethical standards. The contractual arrangement with the outsourced service provider captures these competence requirements and provides the basis for the entity to periodically assess the outsourced service provider's continued commitment to competence.

Example: **Retaining External Tax Assistance**

Compu Services, a developer of analytical software products, currently has limited tax accounting expertise among its staff. The finance director therefore sought to contract with a third-party accounting firm, SMR Ledger, LLP, to review its tax provisions. SMR Ledger is a different accounting firm from the Compu Services auditor.

For successful selection and use of the vendor's services, management was careful to verify that the vendor met the suitability standards set forth in Compu Services' policies. Being directly affected by the quality of the control procedures carried out by the vendor, the CFO spends time with the vendor to understand any assumptions used in models or calculations, particularly as they may impact financial reporting. Indeed, while Compu Services' management chooses to outsource certain tax activities, it remains responsible for the effectiveness of relevant controls regardless of where they are operated. The company therefore requests annual independent certifications of the vendor's internal control effectiveness.

- From pages 85 -86 **Implementing or Assessing Control Activities when Outsourcing to a Third Party**

Approach: **Implementing or Assessing Control Activities when Outsourcing to a Third Party**

The organization outsources some of its operations to a third party, which may or may not issue a "report on controls at a service organization" following an appropriate local or international standard. Although the organization may rely on an outsourced service provider to conduct processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for designing, implementing, and conducting an effective and efficient system of internal control.

Management obtains an understanding of the service organization's activities and whether those activities impact significant classes of transactions, accounts, or disclosures in the company's reporting process. In determining the significance of the service organization's processes to the financial statements, the entity considers the following factors:

- The significance of the transactions or information processed by the service organization to the entity's financial statements
- The risk of material omission and misstatement associated with the assertions affected by the processes of the service organization, including whether the activities involve assets that are susceptible to loss or misappropriation
- The nature and complexity of the services provided by the service organization and whether they are highly standardized and used extensively by many organizations or unique and used only by a few
- The extent to which the entity's processes and control activities interact with those of the service organization

Continue next page……

- The entity's control activities that are applied to the transactions affected by the service organization's activities
- The terms of the contract between the entity and the service organization, and the degree to which authority is delegated to the service organization

If management determines that the service organization's processes are significant to internal control over external financial reporting, then it:

- Identifies the specific control activities performed by the service organization that are relevant to financial statement assertions, and/or
- Selects and develops control activities internally over the activities performed by the service organization.

If a report on controls at a service organization is available, management can use it to determine what financially significant processes are covered, whether appropriate control activities are in place, and what control activities are required in its own organization to address external financial reporting risks.

If an appropriate report does not exist, management can use the entity's own resources, such as internal audit, to review the control activities and ensure that any external financial reporting risks are mitigated by the combination of its own control activities and those of the service organization.

Example: **Obtaining a Report on Controls at a Service Organization from a Service Payroll Provider**

Green Grow Now is a 250-person company that packages and distributes organic produce. It uses a third-party service, Jennssen Inc., to process payroll, which is considered significant to the company's financial reporting because employee costs are a large part of Green Grow Now's expenses.

Jennssen Inc. engages a service auditor to audit its control activities over transaction initiation, processing, and recording, and to issue an SSAE 16 (SOC1)[17] report on controls. When Green Grow Now obtains the report, it assesses whether the described control objectives and control activities performed by Jennssen impact internal control over external financial reporting related to the existence, completeness, and valuation of payroll expense.

Green Grow Now considers the test results in the report and whether any exceptions have been identified. It also considers the period covered by the report and concludes that it needs additional evidence of the operation of control activities for the period not covered. The management communicates directly with Jennssen to inquire about any changes to its processes; Jennssen confirms in writing that no changes have been made.

Based on this information, Green Grow Now concludes that no further action is needed. It also reviews the control activities that it is expected to have in place in its own organization (as specified by the user control activities in the SSAE 16 report) to verify they are implemented and operating as intended.

- From pages 122 -123 **Identifying, Securing, and Retaining Financial Data and Information**

Approach: **Identifying, Securing, and Retaining Financial Data and Information**

Senior IT management establishes policies to define categories of data and assign requirements for securing and retaining the data. These policies support management and employee responsibilities for securing information from unauthorized access or change and for adhering to retention and data destruction requirements. The senior data administrator develops processes and repositories to carry out the data classification policy. Data classification requirements are communicated to personnel responsible for transaction processing through periodic reminders on important internal control responsibilities. Important to this process is considering the benefits and costs to manage and store information and the relative value of the information to the entity.

Example: **Identifying and Protecting Financial Data and Information**

Bio-Adaptive, Inc., a global life science and chemical manufacturer, has developed standard operating procedures to identify, classify, and secure sensitive information, including financial information, throughout the data and information life cycle (input, processing, output, storage). These procedures include, but are not limited to:

Bio-Adaptive, Inc., a global life science and chemical manufacturer, has developed standard operating procedures to identify, classify, and secure financial data and information across the entity and the stages of information life cycle (input, processing, output, storage). As part of these procedures, personnel:

- Confirm adherence to standard operating procedures
- Identify financial data and information that requires restriction of access and retention in order to meet reporting requirements
- Assign appropriate data security categories to sensitive financial data and information when input into the information system
- Review automated application controls that support security, privacy, and storage of financial data and information based on the data security category input
- Review periodically that sensitive financial data and information have been properly categorized[22]

Example: **Identifying and Classifying Data for Financial Reporting**

Freedom Corp., a financial services firm, has a process to tag financial data during transaction processing based on criteria established in the company's data classification policy. Business and IT personnel who are involved in detailed transaction processing are trained in data entry to support accurate and complete classification, tagging, storage, retention, and disposal.

This process reduces the time required to format, organize, and report data. It also enables the company to tag data through eXtensible Business Reporting Language (XBRL). XBRL enables Freedom Corp. to meet certain external financial reporting requirements and to perform comparative analyses to historical, competitor, and projected financial data.

Appendix C: Examples

Below are samples of controls, provided to us by individuals at several organizations, which are used in relation to disclosure management solutions and XBRL. These examples are intended to illustrate possible approaches in managing the risks in these processes.

Disclosure Management Solution

1. On a quarterly basis, the Director of SEC Reporting provides an e-mail to the Controller, confirming that they have reviewed the accuracy and completeness of the HTML (Edgarized) and XBRL formats. This e-mail is then acknowledged by the Controller prior to filing.

2. Annually, we obtain the SOC 1 report from [DISCLOSURE MANAGEMENT SOLUTION NAME] and complete an evaluation template for any reported exceptions.

3. Suggested "complementary user entity controls" are also evaluated and commented on by the financial reporting manager.

4. If needed, we request from [DISCLOSURE MANAGEMENT SOLUTION NAME] a bridge letter that rolls forward the SOC 1 through year-end.

5. User access controls – Annually the SEC reporting manager obtains a listing of all users with access to [DISCLOSURE MANAGEMENT SOLUTION NAME]; and validates whether all users are active employees and should be on the listing.

Appendix C: Examples cont….

XBRL Internal Control Checklist (Taken from Challenges of XBRL report[8])

Planning for new disclosures and tagging changes:

1. Review all current quarter disclosure and any planned tagging changes for appropriate use of U.S. GAAP or extension tags. This includes a review of the tag's preferred label, definition, balance type and negation (if applicable). Extensions should only be created if an equivalent tag cannot be found in the U.S. GAAP taxonomy.

XBRL Tagging Review

1. Level 1 (Block tagging) – includes block tagging of all narratives, tables and footnotes to tables.
    a. Ensure that all narratives, tables and footnotes for a note in the report are included under that note's overall tag (completeness) and appropriately tagged (accuracy for time period)
2. Detail tagging (Level 2 – for Note 1)
    a. Ensure that all required policies in Note 1 are tagged (completeness) and appropriately tagged (accuracy for time period)
    b. Ensure element definitions are correct with regards to the policies the company are reporting
3. Level 3 (Table tagging) – includes block tagging of all tables and footnotes to tables.
    a. Ensure that all tables and table footnotes within a note in the report are tagged to the correct table tag (completeness) and appropriately tagged (accuracy for time period)
4. Detail tagging (Level 4 – for all financial statements and other notes) – includes tagging of all required data in the tables and narratives
    a. Preparer review –
        i. Ensure that all required data in the tables is tagged (completion) and appropriately tagged (accuracy for signage, time period, unit and scale)
        ii. Ensure element definitions are correct with regards to the reported amounts.
        iii. Ensure that all required data in the footnotes to tables and narratives/parenthetical information is properly tagged, including language such as "none" or "no" used to report 0 activity
        iv. Print the view of the rendered file from the disclosure system and file in work paper for independent review.
    b. Independent review –
        i. Review work paper (Printout from disclosure system) for completeness and accuracy of XBRL tags for all required elements
        ii. Ensure that changes identified during the initial planning process we executed according to plan
5. Utilize validation testing system and calculation inconsistencies

[8] http://www.financialexecutives.org/KenticoCMS/Research/catalog/2013/Challenges-with-XBRL.aspx#axzz34RLIJ3F1

Appendix D: Interviews

COSO Board Member

Charles E. Landes is Vice President of Professional Standards and Services at the American Institute of Certified Public Accountants (AICPA)/ COSO Board Member

Mr. Landes shared his thoughts with FERF on the primary intentions of the COSO Board as it released the 2013 Framework. He states, "The first objective was to 'freshen up' the 1992 Framework document. It has been a number of years since COSO issued the original internal control framework, way back before technology was a big player in the whole controls environment, where many controls were done at the manual level. So it was necessary to freshen up the document to read for a current day document." He continues "The second objective of the Board, and certainly one of the higher priorities, was to make clear what a company needs to do in order to have an effective system of internal control, and I believe that was accomplished through the principles that were added to the 2013 Framework. As a result of COSO issuing the small business internal control guidance in 2006, when we first introduced the principles, it was a much more robust document. Not just to read but to understand what was being asked. Building the principles in, around the five mandatory components, made the document easier to understand, implement and determine what does an effective system of internal control look like…"

One of the changes to the new framework included intentionally dropping "financial" from the financial reporting objective by the COSO Board. He states "…because there is a great deal of reporting that occurs today, earnings and other non financial data, a CFO/controller should consider controls around all published reporting, and not merely financial statements in a paper form. Therefore, it is necessary to break down the mentality that other reporting is in a separate silo and not the integrated reporting all together."

As for XBRL, Landes notes, "Users are going to absorb information in greater technological forms than in the past, as it is not a paper world anymore. It is, therefore, important to consider controls addressing where misstatements could electronically occur. For example, if the company has not done a very good job mapping the appropriate general ledger account to the XBRL code, when that is absorbed through XBRL by a user, there may be an error. Why shouldn't companies then subject all reporting to the COSO framework to provide reasonable assurance that the information is correct?"

Another important change from the 1992 Framework, are the controls around OSPs. Landes explains, "CFO needs to understand that even though a function is outsourced to a service organization, the

company is still responsible for their system of internal control. Therefore, there has to be ways that they are monitoring the effectiveness of that service organization. That maybe through service organization reports such as SOC 1 type 2 reports or even meeting with their outside service provider to understand how they assess their risk, and how they make changes to their system. What we tend to see from the audit profession is management thinking - 'this is not something I have to worry about because it is an outside service' - but that is simply not the case; even though the task is outsourced, the company is still ultimately responsible because it is the company's financial statements. Therefore, if the information received is incorrect from the service organization it may impact the company's financial statements. Management must think of ways to monitor the effectiveness of those controls and those processes. The underlying problem with that is all information travels so quickly and at real time, it is difficult to monitor service organizations control because some of information, perhaps around fair value pricing or outsourcing of income taxes, some things happen at the last minute, so management doesn't have time to do an effective job of monitoring and thinking about the risks in advance, and asking oneself *How do I know this information from the service organization is correc*t; *and, what am I doing to control those risks and monitor those control activities?* That is an important item to think about and also difficult. The amount of processes that are outsourced today is very different than it was in 1992…"

In relation to the impact that the 2013 Framework will have on organizations, Landes says, "The framework does not only apply to issuers; it will apply to private, public, governmental, non-profit, etc. that may be interested in designing an effective system of internal control. Whether it is an effective system around their operations, compliance, or reporting (and financial reporting is a subset of that). Furthermore, to answer the question of *impact*, it depends on what your current system of internal control looks like. If your current system of internal control is pretty strong and effective over the years, and has been updated for built in technology controls, I would think that moving from the 1992 Framework to the 2013 Framework, would be relatively painless, ….if, however, your current system of internal control isn't very good to begin with, you are going to have a lot more changes if you are trying to design and operate a system that would be in compliance with 2013 framework. It depends on what your starting point is, and without knowing the starting point, it is hard to determine the gaps you may have and whether the gaps will require major effort to fill, or relatively easy to change controls to fill the gaps."

Audit firms will not need to significantly change their audit methodologies. Landes believes, "…audit methodologies will not change a great deal; I don't expect audit fees will be much higher for an issuer in order to do an integrated audit. However, this assumes the issuer has maintained a good system of quality internal control to begin with. Going back to changes made, COSO believes that the principles

were implicit in the old guidance, what we have done was to lift what was implicit to be explicit by calling it out in 'principles'. If the issuer already had a good system in place, there is going to be a little bit of methodology change. Once methodology changes are made, the audit costs should not be much more, because the principles are already implicit in what the auditors should have already been testing for." In regards to the PCAOB, he adds, "what the PCAOB does with the new framework is up to them, whether the inspection teams will take a 'checklist' mentality, which wasn't the intention, or whether they will want to look at the audit documentation, and go down through each principle and steps that they think may have been necessary. We hope that's not the case. We don't want the audit firm or PCAOB inspectors to view the principles as additional items to put on a checklist and check a box procedure is complete."

The AICPA is also revisiting standards due to the 2013 Framework. Landes states, "We are actually revisiting AICPA standards for auditing of non-issuers (private) to determine whether or not our risk assessment standards need enhancing as well. By that I mean, risk assessment standards directing an auditor when planning their engagement, an auditor has to understand the client's environment, which includes understanding a client's system internal control. Understanding the internal control of a company will help an auditor identify potential areas for misstatements, in other words, the weaker a client's system of internal control is, the higher the chance there could be a material misstatement to the financial statements. Where there is higher risk of potential misstatements, more work needs to be done by the auditor. We don't think our standards will change, but where we will probably address this change in our audit guides where we get more specific to the internal control framework."

Landes expects that companies that do not adopt the required framework in the allotted time may get a letter from the SEC. The CFO should expect the audit committee to get a call from their auditors. He adds, "…it is interesting to consider whether an auditor will consider the non-adoption as a material weakness?" He explains, "If the framework is better and easier to use and understand, but a company chooses to ignore the new framework, an auditor should consider what the decision says about the control environment and how serious is management about an effective system of internal control and shouldn't let that attitude translate to a control deficiency. There may be facts and circumstances that may justify why the company has not adopted, but if is a blatant disregard on the part of the company - that is a clear red flag on the control environment of the company…"

Landes provided some takeaways on the 2013 Framework for CFOs to consider. He indicates, "Since the COSO framework starts with the tone at the top, CFOs, should assemble a cross-functional team to own the conversion. Also, the CFO needs to be serious about making this priority and believe that

the adoption of the new framework will result in a better system of internal controls which will ultimately reduce the risk of material misstatements. The lack of compliance may be embarrassing to a company's reputation and the company's ability to raise money in the capital markets. To me, it is an easy decision for a CFO."

Auditors:

Chuck Harris - Partner, National Auditing Services PwC, LLP

Chuck Harris says that the impact would depend on the company. He explains, "The impact of the 2013 Framework on a company will depend on how well the company understood and implemented the 1992 framework; that is, if management fully understood the principles implicit in the 1992 framework, there shouldn't be a significant impact in transitioning to the 2013 Framework. The articulation of seventeen principles and their associated points of focus provide management the opportunity to assess more effectively the controls in place to effect each principle, possibly requiring management to either revise existing controls or to design and implement new controls. Furthermore, I think where companies, especially public companies, will spend most of their time will be on the components of control environment, risk assessment, information and communication, and monitoring activities. The reason is that companies have a fairly mature system around control activities because of SOX but perhaps less so with respect to these other components of internal control.

When asked whether his clients are experiencing gaps as a result of their assessment of the new framework, Harris shares "…gaps may be too strong of a word…I point to the four components above because those are the components that management is less familiar with; and the principles and the points of focus articulate important aspects of the controls that need to be in place for those principles to be present and functioning. Management's assessment may result in some "tweaking" of its system of internal control. Take risk assessment, for example, management is likely performing some form of risk assessment periodically, but the documentation around the risk assessment process is probably not as strong or robust as it may need to be, to comply with the risk assessment principles in the 2013 Framework."

Harris shared that when an auditor is required to opine on the system of internal control, the auditor will be examining evidence that all seventeen principles are present and functioning. "When we opine on internal control, we make sure that all seventeen principles are present and functioning and gather the appropriate evidence to support our conclusions. Auditors will most likely continue to

focus the majority of their time and attention on control activities. The reason for this is that control activities directly affect whether management can prevent, or detect and correct on a timely basis, potential material errors in the completeness and accuracy of the information reported in the company's financial statements."

In regards to implementing the 2013 Framework, Harris suggests to senior-level financial executives: "Think about making the transition before the auditors come in to begin their audit, because you want to transition with sufficient time to test whether any new controls that are relevant for financial reporting that you needed to implement have sufficient time to operate so you can conclude that they are operating effectively; but more importantly, you should avoid having your auditors begin their audit process under one framework and concluding it under the updated framework. In other words, you don't want your auditors to commence their interim testing when you are on the 1992 Framework; and then you subsequently make changes to your controls based on transitioning to the 2013 Framework which may require the auditor to retest controls or scope in new controls. That is potentially very inefficient and could, depending on the number of changes, be more expensive than it needed to be. The message is go ahead and make transition with two goals in mind: First, give new controls implemented upon transition enough time to operate so that management can conclude on effectiveness; and second, as I indicated above, make this transition before the auditors come in and conduct their initial testing. Remember, auditors cannot tell management what internal control framework to use – they can only audit the system of internal control that management has put in place."

As it relates to DMS, Harris explains the concept of 'upstream and downstream' and how this concept will determine whether DMS will be in scope or out of scope of an audit. He explains, "A company that implements a DMS still has the responsibility of ensuring that there are controls relevant to the solution; but depending on how DMS is used, those controls may not be relevant to the audit. "*Upstream*" implementations are those where DMS pulls information from the company's trial balance, ledgers and/or consolidation systems to generate the company's financial information to comply with regulatory requirements for external financial reporting*, and will require the auditor to consider the controls around DMS* because the direct output now has a bearing on the audit. If that DMS is '*downstream'*, which means the company does not use DMS to compile the required information to comply with regulatory financial reporting requirements, then the auditor has no responsibility to evaluate controls in connection with the audit. That is not to say that DMS or the information it produces is not important, or that management does not have an obligation to design and implement controls over the accuracy and completeness of the information input to or produced from DMS. Management has responsibility for such controls, but from an audit perspective, those

controls occur downstream from the systems that produce the financially relevant information and disclosures for purposes of regulatory financial reporting; and thus, are not part of the audit at this time. The question the auditor will ask is how the disclosure management solution figures into the processing of information that goes into the financial statements. If it is the principle software that produces management's financial statements and footnotes for SEC or other compliance requirements, then DMS will clearly have audit implications.

Harris also shares that controls around XBRL are important. He explains, "There are two aspects to XBRL. The first is from management's standpoint. I absolutely strongly believe that management should have controls around the XBRL reporting process and that those controls should be designed to ensure management's XBRL data is complete and accurate. The second aspect is from the auditor's standpoint. As of now, there is no regulatory requirement for the auditor to be involved in the tagging process or the reporting process for XBRL. Management may certainly engage the auditor at its discretion to test the accuracy of its interactive data as a project unrelated to the audit, but is not required to do so. Until that requirement changes, it is not going to be an audit driven event. Companies run a significant risk if management is not producing accurate XBRL information. For example, an analyst using inaccurate XBRL information may draw wrong conclusions about a company's financial position or results of operations. This, in turn, could damage a company's reputation which, in a competitive marketplace, could have serious implications. This potential scenario once again underscores the importance of management implementing effective internal control over its interactive data process."

Regarding public companies not adopting the new framework in a timely manner, Harris states "I would encourage financial executives of public companies who are thinking about not transitioning to the new framework to consider what management's response would be to a possible comment letter from the SEC as to how its use of a superseded framework satisfies the SEC's criteria for selecting an internal control framework. There really is no bright line when the SEC will begin to question companies that stay on the 1992 framework, but the SEC has stated publicly that it will monitor transition."

Jeff Getz and Sandra Herrygers, Partners at Deloitte & Touche LLP

Both Jeff Getz and Sandra Herrygers believe that the impact of implementing the 2013 COSO Framework in the context of reporting on Internal Control over Financial Reporting (ICFR) depends on where a company's ICFR is today. Getz explains, "Companies may need to consider the seventeen

explicit principles that underlay the existing five components from the 1992 Framework. These seventeen principles are significant because the 2013 Framework requires them to be present and functioning for the company to get a passing grade." Herrygers agrees and adds, "Whether there are gaps to be addressed may vary depending on how well a company constructed and maintained its ICFR under the old Framework."

Getz and Herrygers highlighted a few of the more significant content enhancements in the 2013 COSO Framework. "There is a new focus on the risk assessment component," Getz states, "which is key, because if your risk assessment is inadequate, then you likely have deficiencies in your controls. In particular, fraud risk assessment is called out as a separate principle in the new Framework, but wasn't as prominent in the 1992 Framework. Another risk assessment principle present relates to the timely assessment of risks that may affect the business and ICFR; for example, an acquisition, a system implementation, or changes in key personnel."

Herrygers comments, "These principles may require companies to improve documentation and controls, although many larger companies may have already been focusing on fraud risk assessments." Getz enforces the notion that companies really cannot spend enough time thinking about fraud. "Fraud was the primary driver for the requirement to report on ICFR under Sarbanes-Oxley," he says, "and fraudulent financial reporting still continues to occur today."

Getz points out that a second significant area of focus in the new COSO Framework is information technology (IT). "The IT context in the 1992 Framework was light," he says, "so much so that management looked to other frameworks, such as COBIT[9], for considerations." Herrygers adds, "COBIT had a SOX for COBIT[10] guide, which many companies and auditors leveraged for IT concepts. The new COSO Framework embedded many of the same concepts. So even though there is additional content related to IT in the new COSO Framework, it may not be an area of significant change for companies that have already included those controls in their ICFR program."

Getz emphasizes that the 2013 Framework includes significant changes related to the use of OSPs. "The use of external service providers is more common today, so COSO provided explicit content related to OSPs in 12 of the 17 principles. The underlying idea is that an entity's responsibility for controls extends to the activities performed on their behalf by OSPs. Therefore, a company should understand the OSP's activities and processes to be able to analyze the risks and help ensure that the

[9] Control Objectives for Information and related Technology (COBIT®), developed by ISACA®.

[10] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Sarbanes-Oxley-2nd-Edition.aspx

appropriate controls are in place regarding those activities–whether performed by the OSP or by the company," he says.

"Since a deficiency in an OSP's controls may be indicative of a deficiency in the company's controls," he states, "management should not depend solely on receiving a Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, (SSAE 16) report later in the year. Instead, companies should be proactively monitoring their OSPs throughout the year to make sure there are no surprises at the last minute."

"However, the extent of certain OSP monitoring depends on how significant the OSP's activities are to the company; for example, only outsourcing processing payroll versus outsourcing entire IT systems," Getz states. "Similarly, when a company engages a new OSP, the risk assessment should help analyze whether this new relationship poses a higher risk. If it does pose a higher risk, companies should consider what additional activities should be implemented to more proactively monitor the OSP's performance," he says. Herrygers expands on the use of OSPs, "There wasn't much content on OSPs in the 1992 Framework, and some companies focused on getting service auditor's reports related to the control activities in place at the OSPs. Today, however, there is much more context in the 2013 Framework related to the other components—well beyond the control activity component to the OSP."

"Some of these considerations may be satisfied through a service auditor report, but there are others that require more specific monitoring from the company," Herrygers says. "As an example, one of the points in the 2013 Framework related to the fraud risk assessment principle is that a company should consider the risk of fraud related to outsourced activities as a part of their fraud risk assessment. This assessment should be done by the company—it is not something that the company will look for in a service auditor's report. So, it is really important that companies go through the various consideration points in each of the components and consider how to address them— whether through monitoring activities by the user organization or through a service auditor's report on the OSP," Herrygers concludes.

"Lastly, the quality and reliability of the information that management uses in their ICFR may be much more explicit, which may be in direct response to the evolution of how information is used in ICFR. Information today comes in a number of forms, but two most typical are IT system generated information, which is typically subject to the IT controls, and other ad-hoc data and reports outside of the IT systems, (e.g., data warehouses, Excel spreadsheets and query tools) which have a higher risk of error. How does the company ensure that the information is reliable?" Getz asks.

Herrygers recommends that companies perform a 'gap assessment' by mapping their current controls to the seventeen principles, and by considering the points of focus for each principle, to identify potential gaps. She explains, "In some cases, the principles are more specific and prescriptive about what companies need to have in place to demonstrate that they have addressed a principle. Performing the gap assessment may help companies:

1) Identify the need to scope in other already existing controls; i.e., the company identifies a gap, but has other existing controls that were not assessed under the prior Framework;
2) Enhance existing controls, i.e., a company might have a control in place related to the principle, but it may not address all the specific attributes that are relevant and, thus, may need to be enhanced; and
3) Design and implement new controls to achieve the principle.

Both Getz and Herrygers recommend companies focus their energies on the areas where there is new or enhanced content in the 2013 Framework. "We do not anticipate a situation where a majority of companies have a gap in a principle, as gaps are expected to be very company-specific based on their circumstances. For example, companies that make extensive use of OSPs may find some gaps related to controls over their portfolio of OSPs, while other companies, particularly the mid- to smaller-sized companies, may find some tidying up to do with delegation of authority, or assessing and monitoring the competence of the groups that are preparing the financial statements and applying GAAP. We suggest companies also look closely at the common areas of material weakness and/or fraud, and as they are looking at the new Framework, focus on those areas and make sure the controls are appropriate. So regardless of your view of the potential impact of the new Framework…this is an opportunity for management to take a 'fresh look' and challenge, in the spirit of a new Framework, whether they have the right controls place."

Getz and Herrygers identified principles that they believe may be particularly challenging for many companies. For example, principle number five, which deals with establishing accountability for internal control; principle twelve, which deals with establishing expectations for performing controls which the Framework links to maintaining internal control policy and procedures. Getz suggests, "Many organizations may not have been maintaining policies and procedures to achieve the principle, which may be a gap. Principles five and twelve work in tandem, and management needs to establish policies and procedures for its employees and then hold them accountable for those responsibilities."

Herrygers points out that her preferred principles are no. 11 *Selecting and developing general controls over technology*, and no. 13, *Use of relevant information to support the functioning of*

internal control. While many companies have general IT controls in place today, there is opportunity to improve the linkage between financial statement risk and the automated controls and information used in business controls to address risks. There is also opportunity for companies to improve the use of access controls to help segregate duties related to business transaction processing, which helps mitigate the opportunity for fraud.

Getz and Herrygers agree that the 2013 Framework is a great tool for management to use to take a fresh look at their entity level controls and at their process level and IT controls as well. The new COSO Framework gives companies the opportunity to look a little closer at the controls currently in place and determine whether they are really addressing their financial reporting risks.

Chris Jeffrey, CPA, Partner, Risk and Internal Audit Consulting Services practice at Baker Tilly

Chris Jeffrey believes that the new framework is a great improvement over the 1992 Framework, "…mainly because the 1992 framework was quite nebulous and left a lot to interpretation. While the new framework is still intended to be principles based, the addition of the 17 principles with the points of focus underneath that, provide actionable steps that a company can take to implement their controls framework to get a better understanding. At the end of the day, it is going to be highly useful for companies that plan to implement their framework from the ground up to use the compendium of examples and get a better understanding what the principles and points of focus are driving at."

Jeffrey also believes that companies should consider the implementation of this framework as an opportunity for improvement rather than just a mapping exercise. He says, "For companies that already have a formal internal control framework in place, such as those companies that are already compliant with Sarbanes Oxley, there will be some mapping, but if they only consider this as a mapping or compliance exercise, they are missing an opportunity to take a look at their control environment to make some value-added changes based on the new framework. This new framework is very dynamic."

It seems that the COSO framework is 'catching up' with companies that are already SOX compliant, Jeffrey explains, "…as I reviewed the points of focus and more detail in the compendium, COSO calls our certain items such as outside service providers, risk assessment and information technology, but overall it seems that COSO is catching up with companies that already have a robust control environment in place since SOX has been in place for over ten years."

In regards to complying with the 2013 Framework on the date of transition, Jeffrey states, "The SEC is very clear that you don't have to use the COSO framework to comply with SOX; but, practically speaking, most companies do use the COSO framework. Regardless, its implementation will be heavily monitored by most company's external auditors. Since I am on the advisory side of the firm, my team is working closely with our client's external auditors. Therefore, I know they will be looking at whether a company has actually done enough work around the implementation of the new framework. Since this is not intended to be a 'check the box' exercise for companies, external auditors are looking to ensure companies are taking this seriously."

Of the five COSO components, Jeffrey believes there will be a lot of focus within the control activities and monitoring sections. He says "…the real work will be for companies to look at their controls framework, understand where the new principles are and make sure that they are covered. So the value of the new framework to a company comes in understanding where they have gaps, and conversely, understanding areas where they might be 'over controlled' and trying to reconfigure their control framework based on their assessment." In regards to the level of work companies need to do to become compliant with the new framework, Jeffrey shares, "…. Since most companies that are SOX compliant are already dealing with risk assessment, IT and outside service provider controls, the transition will be to ensure that a company has the principles covered within those areas. For instance, there could be more work in around outside IT service providers. For example, "…we were working for a client that outsourced an IT function, and they chose to outsource to an IT service provider that did not have a SOC 1 report in place – we helped that company put mitigating controls in place that ultimately addressed the new COSO principles. However it wasn't a simple task. The framework is clear that companies need to do their diligence around selecting an outside service provider and to make sure they select the right outside service providers that have appropriate controls in place, especially if the company needs to be SOX compliant. If an OSP does not have appropriate controls and cannot demonstrate the operation of those controls (such as in a SOC 1 report), I would recommend to my client not to use that OSP. "

For non-SEC registrants, Jeffrey states "…auditors will continue to look at their client's control environments to comply with the AICPA's 'risk assessment standards'. However, if an auditor chooses to rely on the controls of their client to reduce their substantive testing they may be more inclined to do so if the new COSO framework was in place. If non-SEC registrants do comply with the new COSO framework and do go through the transition process, they may have a better argument to push their auditors to rely on their controls, which could result in a reduction in audit fees."

For SEC registrants, Jeffrey explains "…auditors will take a good hard look at what a company's efforts were over the company's implementation period to ensure that the company has gone through a robust exercise to implement the new COSO framework. I don't see that auditors will select one area in particular to focus on; all of the principles will need to be covered. It will be helpful for companies to create or use a tool to assist with their transition, as this can be used evidence to auditors that a robust implementation has been completed."

Management:

J. Stephen McNally, Finance Director, Campbell Soup Company

As IMA's[11] representative on the COSO Internal Control Framework Refresh Project Advisory Council and author of *The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition*[12], J. Stephen McNally suggests that companies need to begin by "…educating the core team on the 2013 Framework…to identify how the updated edition is the same as and different from the original … and how the updated framework will potentially impact the company's current SOX program. This can be done by mapping existing controls against the 2013 Framework." He reiterates the sentiments of COSO's Board members, "…if a company interpreted the 1992 Framework correctly, the new Framework will have little impact on a company's underlying controls. Furthermore, if there is a deficiency or gap relative to the 2013 Framework, it is likely that a company also had a deficiency under the 1992 Framework, too. You may have interpreted the old Framework incorrectly. "

As it relates to gaps that could be detected, McNally suggests that it all depends on the maturity level of the company's processes around internal controls and explains "…companies that were mature in their inventory control process or inventory control environment in the past should not see many changes and/or have a hard time transitioning. With that said, the original framework was very wordy and perhaps difficult at times understand, making it hard to extract the important nuggets of insight."

The new Framework provides many benefits. McNally thinks the enhancement "…will encompass key changes that have occurred in businesses over the past 20 years, such as globalization, growing regulatory requirements, more complex business models, including the use of outside service providers in a much more significant way, greater reliance on technology, higher stakeholder expectations regarding the board and the board's oversight of risk management, identification of

[11] Institute of Management Accountants, Inc.

[12] http://www.coso.org/documents/coso%20mcnallytransition%20article-final%20coso%20version%20proof_5-31-13.pdf

fraudulent activities, etc.…" Also the updated framework is more user friendly, McNally continues "…under the old Framework, the internal control principles and supporting points of focus, or key consideration to think about, were embedded throughout, whereas in the updated Framework, the principles have been codified and the requirements for effective internal control have been clarified. Management now has clarity that, to conclude they have an effective system of internal control, all seventeen principles must be present and functioning, and the five components of internal control must all be present, functioning and operating together in an integrated manner. And now management has additional help in making their assessment via the supporting points of focus, which have been called out in a clear and concise way. If a company cannot say that their internal controls, specifically the seventeen principles, are present and functioning, their system of internal control may not be effective."

In regards to technology, McNally explains "…the new framework recognizes that technology is now a key part of controls going forward. Specifically, in the Control Activities component, principles no. 11 reads 'the organization selects and develops general controls over technology to support the achievement of objectives.' Another perspective is how technology plays a role with the fifth component, Monitoring Activities and explains, "During the COSO Advisory Council meetings, there was discussion around what monitoring looks like. Initially, it seemed that monitoring activities were heavily weighted to internal and external audits. However, technology allows us to do some real time monitoring, through mechanisms like dash boards, comparing transaction details to predetermined thresholds for anomalies, monitoring trends and patterns that may raise red flags, and assessing performance via metrics. Technology overall allows for deeper and more streamlined monitoring than in the past and allows companies to embed internal control responsibility into the fabric of their culture, business processes and procedures, which was not as evident in the past."

To make the transition easier, the COSO board published, as part of the overall Framework materials, a volume entitled *Illustrative Tool for Assessing Effectiveness of a System of Internal Control*. McNally states, "…COSO published this document to assist users when assessing effectiveness of internal control, providing both illustrative templates as well as scenarios illustrating how to use these templates. COSO also issued "*Internal Controls Over Financial Reporting: A Compendium of Approaches and Examples*", which McNally states was "…issued in conjunction with the Framework which is considered separate but complimentary to it. It is meant to guide those who leveraged the original Framework for external financial reporting purposes and/or others that will do so going forward. It provides a lot of good ideas on how to leverage the Framework and what controls can look like from a financial reporting perspective. It is a very user friendly resource, allowing you to pinpoint what insight you are looking for versus reading the document cover-to-cover."

McNally shares that "…back in 2000, the easiest component to implement, document and test was the *Control Activities* component. However, there were four other components in the COSO framework and they also had to be addressed under SOX 404 requirements. The four remaining components - *Control Environment, Risk Assessment, Information & Communication,* and *Monitoring Activities* - are tougher to address and evidence. For example, Control Environment principle no. 1 reads 'the organization demonstrates a commitment to integrity and ethical values'. How does a company do this? Is there a documented code of conduct? And even if yes, how do you document that the company is complying with the code of conduct? This is where management's judgment and creativity come in. Perhaps in this case, management can leverage technology. For example, requiring employees to take an on-line course on their company's code of conduct; and then have them confirm that they have read and are complying with it. Leveraging the supporting points of focus in the framework, as well as, the approaches and examples in the supporting Compendium, can help management effectively address all five components of internal control."

McNally's final thoughts around the benefits of the new framework, "…besides supporting management at public companies in meeting their SOX compliance requirements, the new Framework can and should be leveraged throughout the organization - at the division, business unit, and/or functional level - to mitigate risk related to the achievement of operational, reporting and compliance objectives. The 2013 edition of COSO's Framework can provide a common language regarding governance, risk management and internal control."

Keith Kawashima Managing Director, Internal Audit Services for Protiviti Inc.

Speaking from his client's perspective, Keith Kawashima indicates ,"…the largest impact that the 2013 Framework will have on clients is in the area related to internal control over financial reporting. Most, if not all companies state in their financial statement that they use the COSO framework to evaluate the effectiveness of internal control over financial."

Regarding changes in controls, Kawashima states "The 1992 Framework was solid and a good way to evaluate controls. If you compare the two, the 2013 version gives additional guidance and more specificity to the framework than the 1992 version. The same five components exist, but what is new is the seventeen principles and related points of focus that now align with the components within the framework. These nuances give users of the framework a lot more guidance around what constitutes an effective control environment. Another significant change is that the revised Framework makes is clear that all of the seventeen principles should be present and functioning, as well as, operating together."

He explains, "The biggest gap that many of my clients have experienced is the need for additional documentation. With the additional specificity that is contained in the new Framework, my clients have had to update or add documentation to reflect or clarify controls that, in many instances, the company was already performing. For example, the added guidance around entity level controls may require more or greater clarification of the documentation of the related control activities."

In regard to principles being present and functioning, Kawashima shares "…principles should be evident in their own component. A good example is the COSO component of *Control Environment* which has five principles defined for it. All five are required to be present and functioning. Each principle may have a number of controls in place that help to support it. As an example that demonstrates the fourth principle under control environment *Demonstrates commitment to competence*, you would expect to see company control activities including company policies and procedures documenting, a detailed job requisition, and the need to define specific job responsibilities. You would also look at what the company does in recruiting, such as background checks, a defined hiring process which may include validation of education milestones such as transcripts or certifications, or contacting of referrals if appropriate. You would also expect to see ongoing performance evaluations and for some positions these activities might include relevant training or professional development.

Defining 'present', would be the evaluation of whether the design of the controls is appropriate to effectively support the specific principles and 'functioning' is the evaluation of whether those controls are operating effectively. Within SOX and internal audit world, testing of the controls in place is performed; and, if the right control activities are in place and they are operating effectively, one can than conclude, they are present and functioning. Most of these controls are already in place for most companies, but the new Framework gives more in depth guidance around them. The new Framework also discusses other areas that most companies will, at a minimum, need to do more to document existing controls and for some, may require new controls to be put in place. Common areas where we are seeing need for additional controls or clarification and documentation of existing controls are in areas such as entity level controls, information technology and outside service providers."

As it relates to a company's auditors, Kawashima notes "…what we see happening is the culmination of a few things. First, over the last couple of years, there has been an ongoing scrutiny by the PCAOB of the work that external audit firms perform. The PCAOB inspects some of the audits that the firm completed, the conclusions that the firm came to and the support for those conclusions and produces an inspection report, which highlight whether the work done by the external auditor supports and substantiates conclusions made by the external auditor. Some of the common areas

listed where evidence was deemed to be insufficient and would require external auditors to gather more data to support their conclusions include reliance on work of others, management review controls, IT controls, etc. Then, if you add to that the introduction of the revised COSO framework, it is easy to see that the efforts for most companies and their external auditors may continue to grow around the evaluation of internal controls over financial reporting.

Besides providing the appropriate evidence to auditors to complete audits properly, other benefits that Kawashima is finding is that companies "…have the opportunity to rationalize controls with the refresh and highlight those that really matter. Also, they can now reduce controls that are not as important to organization to achieve…this is causing companies to review control by control and take a hard look at where they all fit in…"

As part of the overall submission of financial reports, Kawashima explains "…if you didn't have the right controls in place in the last stage, and a defined process and supporting tools to allow for timely and accurate submission of the company's required information to the SEC for these various reports, a company can potentially put themselves at risk. There continues to be a growing focus around controls that are in place over the submission of reports, including XBRL exhibits, to the SEC, or any other regulatory bodies for that matter. As the requests of these regulatory bodies are expanding, controls should expand as well."

Disclosure management solutions are also an area where controls are needed, he explains, "… this is certainly an area where *garbage in garbage out* applies. If you don't have a control around the DMS to identify disclosure events and transition, no process in place to support those disclosures, and monitor what you are disclosing; then, a company runs the risk of doing it incorrectly. Whether under the old or the new revised framework, a company must have a process in place to ensure that they are doing it right and are consistent."

Director of Internal Audit of a Fortune 500 Insurance Company

Even though this Fortune 500 insurance Company is at the midpoint of their implementation of the new Framework, its director of internal audit shares "…the new framework has impacted their SOX 404 guidance and identified any gaps in control documentation. We have a project plan in place to address any gaps." "The gaps where solely a documentation to reflect the points of focus that is within the new framework and an exercise to complete the documentation and assessment process in light of how the rest of our SOX documentation works. The explicit points of focus where very helpful in understanding the intent of the controls."

In relation to process, "We have a data base and standards of how those controls need to be described and then the assessment process on top of it….to comply with SOX 404 requirements. Even though it is a subtle distinction, the control processes themselves, are documented and understood; it is just that additional step that we do to facilitate the SOX 404 assessment that had not been done…which we have changed under the new Framework…" For example, the company found a documentation gap in the Control environment space. The director explains, "…we have code of ethics procedures in place for annual compliance for employees, under the old Framework we had high level reference, and less rigor in our SOX 404 compliance documentation; however, under the new Framework, we are documenting more detail in our SOX 404 compliance to clearly draw a line of sight as to how our code of ethics procedure are meeting the COSO principles, using the points of focus to best document it."

The director expects the new Framework to have future benefits of applicability beyond the SOX based compliance. He explains "…we want to use a similar approach to the framework in order to provide additional transparency to ourselves, regulators, senior leaders, etc. on how the system of internal controls work holistically, and giving the company a common language on internal controls."

"So far, there has not been so many challenge around financial reporting objectives, because we are finding that we already have the control processes and governance process in place already", the director explains, "it is only documentation of these process."

Regarding outside service providers, the company is now taking a closer look at SSAE 16 reports from OSP and identifying areas where the audit report does not cover specific control expectations, and determining how else the OSP can evidence that for the company.

The director notes that "..In October 2013, the PCAOB issued the *Staff Audit Practice Alert No. 11 - Considerations for Audits of Internal Control Over Reporting*[13] (alert), provides some clear direction to all the public accounting firms of the PCAOB expectations around the auditing that is performed on certain control types. This alert includes, for instance, IT controls, management review controls, etc. The alert is in line with the new COSO framework, but a bit more prescriptive because this is what they will be expecting of auditors, therefore, we are using as well to update our documentation."

[13] http://pcaobus.org/Standards/QandA/10-24-2013_SAPA_11.pdf

Managing Director of a Fortune 500 Technology Company

As it relates to the impact of the 2013 Framework, the managing director indicates that "Our mapping exercise of our existing SOX risks and controls to the seventeen principles identified very few gaps. The gaps were primarily documentation issues where we have existing controls but have not included them in our SOX design. These were primarily entity level controls."

It was also stated that "The principles put more structure and define better what is meant underneath the different components. For example, the explanation of areas to consider under risk assessment will help companies think more broadly around potential risk areas like emerging markets, the impact of IT in their controls framework and fraud risk. The framework also requires a stronger linkage across areas. For example, if there is an issue with an IT General Control, the company needs to clearly examine and document the potential impact to their control activities related to that IT area deficiency. For many companies who have been updating their risk assessments and controls design on a fairly rigorous basis over the past ten plus years, this will be more of a mapping exercise with some additional controls wrapped around the core design."

Concerning the benefits that the 2013 Framework provides, "The 2013 Framework has pushed us to evaluate our design against a deeper set of assumptions and requirements. It has reconfirmed our guiding principles to think broadly and deeply across the business to make sure we are considering all areas that impact the accuracy and completeness of our financial reporting and areas that present the risk of financial fraud within the business. "Furthermore, we have other areas of our business that operate compliance programs but leverage other frameworks (i.e., Five Elements of Compliance and Seven Essential Elements of Compliance.) The expansion of the 2013 Framework into the seventeen principles helps us better align our SOX system of internal controls with these other compliance frameworks. This increases our ability to quickly identify the common elements between our SOX program and these other compliance programs and enable these other programs to leverage our core design as the foundation for their design."

As for OSPs, "Currently our process is to survey our controllers and other stakeholders every year to reconfirm where we are leveraging outside service providers for areas that impact financial reporting and ensure that we, as a company, are receiving audit reports which address critical control requirements, reviewing those reports for deficiencies and putting mitigating controls in place for any deficiencies which may occur. We address risks within processes and systems our outsource providers as if they were internal departments."

About RR Donnelley Financial Services

A Fortune 300 company, RR Donnelley is a global provider of financial disclosure solutions, helping our clients efficiently meet their regulatory obligations and streamline their SEC reporting process. With a global network of service professionals and innovative technology, RR Donnelley is uniquely positioned to assist companies with all of their financial communications needs. RR Donnelley provides:

- **EDGAR Filing Expertise** - Handling more than 130,000 SEC filings annually - 10-K, 10-Q, DEF14A, 8-K, S-1, S-4, S-3 – more than any other filing agent
- **XBRL Filing Experience** - Tagging more than 35,000 SEC filings to date, including transactional registration statements requiring XBRL
- **Deal Leadership** - Bringing the world's largest financial transactions to market – IPOs, merger acquisitions, bankruptcy/restructuring, leveraged buyout transactions
- **Venue® Virtual Data Rooms**- Providing secure document storage – facilitating Regulatory Compliance activities, M&A Due Diligence, Fundraising & LP reporting, Board of Director communications and IPOs
- **ActiveDisclosure** - Built around Microsoft Office® productivity tools, RR Donnelley's comprehensive disclosure management solutions works the way you do.
- **Extensive Distribution Network** - Delivering content across 14 time zones, 4 continents, and nearly 40 countries
- **Financial Stability** - A $10.6 billion Fortune 500 company founded in 1864

For more information, visit:

www.financial.rrd.com

RR DONNELLEY

www.activedisclosure.com

RRD ActiveDisclosure℠

www.venue.rrd.com

RR DONNELLEY VENUE

About the Authors:

Ray Purcell is a CPA with over 30 years in various finance leadership roles in industry, with experience in controllership, business process redesign, shared services, and internal controls. For most of his career, Ray worked in the industrial gases industry. He served as U.S. controller of BOC Gases, a division of The BOC Group plc. In 2001, he moved to Honeywell and played a leadership role in the shared services organization, with responsibility for accounting services in the United States and Mexico.

Since 2005, Ray has been with Pfizer, where his focus has been on SOX compliance and financial controls. In that role, he has recently played a significant role in the development and implementation of a new governance, risk, controls and compliance function at Pfizer, and leads the center of excellence for financial controls within that organization. The views expressed in this paper are based on the interviews and should not be interpreted as reflecting the views or policies of Pfizer.

Ray has participated in several FEI/COSO working groups, including the group that reviewed and commented on the COSO Guidance on Monitoring Internal Control Systems. He served as the FEI representative on the Advisory Council to the COSO project to update the 1992 Internal Controls – Integrated Framework, and chaired FEI's Working Group on the framework project. Since 2013, Ray has also served as a Trustee of the Financial Executives Research Foundation (FERF), with leadership of the FERF Development Committee.

Leena Roselli is Senior Manager, Research at Financial Executives Research Foundation, Inc. (FERF). She received her Master's of Business Administration degree from the Saint Peter's University. Prior to joining FERF, Leena held technical accounting research positions in the pharmaceutical, insurance and retail industries. She can be reached at lroselli@financialexecutives.org or 973-765-1039.

The authors have worked to accurately present the comments of the interviewees; the views expressed in this paper are either those of the authors or of the interviewees, and do not necessarily reflect the views or policies of FEI or Pfizer.

Acknowledgements

A research project of this nature is dependent upon the cooperation and support of financial executives and experts who are willing to share their experiences for the benefit of others. FERF is overwhelmed by the willingness of our six interviewees named below and two interviewees who participated anonymously, to provide an understanding of the impacts that companies will experience during the 2013 COSO Framework transition. Special thanks to the following individuals for their participation on this report:

- Charles E. Landes - COSO Board Member, and Vice President of Professional Standards and Services at the American Institute of Certified Public Accountants (AICPA)
- Charles E. Harris - Audit Partner at PwC, LLP, Auditing Services Methods & Tools
- Jeff Getz and Sandra Herrygers - Audit Partners at Deloitte & Touche LLP -
- Chris Jeffrey - Audit Partner at Baker Tilly, Risk and Internal Audit Consulting Services
- Stephen McNally - Finance Director at Campbell Soup Company, IMA[14] representative to COSO Advisory Council.
- Keith Kawashima - Managing Director at Protiviti Inc., Internal Audit Services

Thank you to RR Donnelley for sponsoring the report.

[14] Institute of Management Accountants, Inc.

About Financial Executives Research Foundation, Inc.

Financial Executives Research Foundation (FERF) is the non-profit 501(c)(3) research affiliate of Financial Executives International (FEI). FERF researchers identify key financial issues and develop impartial, timely research reports for FEI members and non-members alike, in a variety of publication formats. FERF relies primarily on voluntary tax-deductible contributions from corporations and individuals. Questions about FERF can be directed to bsinnett@financialexecutives.org. The views set forth in this publication are those of the author and do not necessarily represent those of the FERF Board as a whole, individual trustees, employees, or the members of the Advisory Committee. FERF shall be held harmless against any claims, demands, suits, damages, injuries, costs, or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by the Foundation or any of its representatives. FERF publications can be ordered by logging onto http://www.ferf.org.

International Standard Book Number
978-1-61509-153-9

Printed in the United States of America

First Printing

Financial Executives Research Foundation (FERF) gratefully acknowledges these companies for their longstanding support and generosity

PLATINUM MAJOR GIFT | $50,000 +

Exxon Mobil Corporation
Microsoft Corporation

GOLD PRESIDENT'S CIRCLE | $10,000 - $14,999

Cisco Systems, Inc.
Cummins Inc
Dow Chemical Company
General Electric Co
Wells Fargo & Company

SILVER PRESIDENT'S CIRCLE | $5,000 - $9,999

Apple, Inc.
The Boeing Company
Comcast Corporation
Corning Incorporated
Credit Suisse AG
Dell, Inc.
Duke Energy Corp.
Dupont
Eli Lilly and Company
GM Foundation
Halliburton Company
The Hershey Company
IBM Corporation
Johnson & Johnson
Lockheed Martin, Inc.
McDonald's Corporation
Medtronic, Inc.
Motorola Solutions, Inc.
PepsiCo, Inc.
Pfizer Inc.
Procter & Gamble Co.
Sony Corporation of America
Tenneco
Tyco International Mgmnt Co.
Wal-Mart Stores, Inc.