Deloitte.

Heads Up

September 5, 2014
Volume 21, Issue 23

In This Issue:

Challenges and Leading Practices Related to Implementing COSO's *Internal Control — Integrated Framework*

by Jennifer Burns, Deloitte LLP; and Sandy Herrygers, Deloitte & Touche LLP

Introduction

In response to a confluence of regulatory statements and standard-setting activities (e.g., by COSO,[1] the PCAOB, and the SEC), companies, audit committees, auditors, and regulators have increased their focus on internal control over financial reporting (ICFR). Statements by representatives from the SEC and PCAOB have emphasized that companies and auditors should increase the attention they give to internal control. For example, in a December 2013 speech, SEC Deputy Chief Accountant Brian Croteau stated the following:

> As we maintain or increase the intensity of our focus in [ICFR] . . . I remain convinced that at least some of the PCAOB's inspection findings related to the audits of internal control over financial reporting are likely indicators of similar problems with management's evaluations of ICFR, and thus potentially also indicative of risk for unidentified material weaknesses [and] I continue to question whether all material weaknesses are being properly identified. . . . This could be either because the deficiencies are not being identified in the first instance or otherwise because the severity of deficiencies is not being evaluated appropriately.

And in a March 2014 speech, PCAOB Board Member Jeanette Franzel noted:

> We are currently in a "perfect storm" in the area of internal control over financial reporting, which demands effective action by all participants in the financial reporting and auditing chain. Management, internal auditors, and external auditors will be navigating the updated Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control — Integrated Framework" at the same time that external audit firms are taking steps to respond to PCAOB inspection findings associated with their audits of internal control.

Since COSO issued its *Internal Control — Integrated Framework* (the "2013 Framework") in May 2013,[2] management teams have been taking steps to implement it in accordance with COSO's transition guidance.

Since COSO issued the 2013 Framework, management teams have been taking steps to implement it in accordance with COSO's transition guidance.

While the 2013 Framework's internal control components (i.e., control environment, risk assessment, control activities, information and communication, and monitoring activities) are the same as those in the 1992 Framework, the new framework requires companies to assess whether 17 principles are present and functioning in determining whether their system of internal control is effective. Further, the 17 principles are supported by points of focus, which are important considerations in a company's evaluation of the design and operating effectiveness of controls to address the principles. These changes will drive the need for a different deficiency evaluation process. From an ICFR perspective, when

[1] COSO is the Committee of Sponsoring Organizations of the Treadway Commission. In May 2013, COSO updated its *Internal Control — Integrated Framework*, which was originally issued in 1992.

[2] The 2013 Framework and Illustrative Tools can be purchased from the AICPA Store. An executive summary of the 2013 Framework is available for free on COSO's Web site.

one or more of the 2013 Framework's 17 principles are not present and functioning, a major deficiency exists, which equates to a material weakness under Section 404 of the Sarbanes-Oxley Act of 2002 ("SOX 404").[3] In addition, it is important to recognize that entity-level controls are generally indirectly related to the financial statements and therefore are more difficult to quantitatively evaluate than direct process-level controls. Entity-level controls are also typically more tailored to the size, complexity, and risk profile of the organization and therefore their evaluation is more qualitative.

While companies use COSO's framework in connection with SOX 404 compliance and ICFR, a significant trend has emerged regarding extending its application to other regulatory or operational risks. Overall, companies have both an impetus and an opportunity to use their implementation of the 2013 Framework as a means to objectively reevaluate their internal controls, identify areas of improvement and synergies, and identify opportunities for systematically managing regulatory, operational, and reporting risks.

This *Heads Up* discusses issues related to the timing of implementing the 2013 Framework as well as implementation challenges and leading ICFR practices. It also provides observations and perspectives regarding applying the 2013 Framework for operational and regulatory compliance purposes. See Deloitte's June 10, 2013, *Heads Up* for an overview of the 2013 Framework.

Implementation Timing

Most companies are moving forward with adopting the 2013 Framework this year, in accordance with COSO's transition guidance.

Questions have arisen about whether companies are required to adopt the 2013 Framework in the current year. COSO provided transition guidance that recommends adoption of the 2013 Framework by December 15, 2014, at which time the 1992 Framework will be superseded. The SEC requires companies to use a "suitable, recognized control framework."[4]

Most companies are moving forward with adopting the 2013 Framework this year, in accordance with COSO's transition guidance. They have cited a number of reasons for doing so, including:

- Boards, audit committees, and management teams desire to demonstrate the use of the latest guidance and leading practices from COSO.
- The principles and points of focus used in the 2013 Framework provide a clearer explanation of the components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring activities) than the older framework. Evaluating the state of an organization's internal control against the principles and points of focus may provide value to organizations by streamlining and enhancing the effectiveness of systems of internal control (i.e., mitigating risks).
- Companies do not want to be perceived as being behind their industry peers, which are likely to be adopting in the current year.
- Adopting the 2013 Framework in accordance with COSO's transition guidance may be expected by investors, bankers, industry regulators, and other stakeholders.

These companies have their gap assessment under way right now, with a target to have the gap assessment and initial testing of ICFR completed by the end of the third quarter. This leaves the fourth quarter for remediation of internal control gaps and retesting. This timing helps ensure an efficient and effective ICFR attestation process for management at year-end.

[3] The 2013 Framework contains the following new guidance on a major deficiency in internal control: "When a major deficiency exists, the organization cannot conclude that it has met the requirements for an effective system of internal control. A major deficiency exists in the system of internal control when management determines that a component and one or more relevant principles are not present or functioning or that components are not operating together. A major deficiency in one component cannot be mitigated to an acceptable level by the presence and functioning of another component. Similarly, a major deficiency in a relevant principle cannot be mitigated to an acceptable level by the presence and functioning of other principles."

[4] SEC Exchange Act Rule 13a-15(c).

We have observed some instances in which companies have decided to continue to apply the 1992 Framework for the current calendar year. Their decisions were generally based on consultations with a number of stakeholders, including the board, audit committee, and internal and external auditors. Regardless of their decision, companies should clearly disclose in their annual assessment of ICFR whether they used the 1992 Framework or the 2013 Framework.

Editor's Note: Under SEC rules (17 CFR Section 240.13a-15(c)), the "framework on which management's evaluation of the issuer's internal control over financial reporting is based must be a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment."

PCAOB Auditing Standard 5[5] states that the "auditor should use the same suitable, recognized control framework to perform his or her audit of internal control over financial reporting as management uses for its annual evaluation of the effectiveness of the company's internal control over financial reporting." As a result, the timing of when the auditor makes the transition to the 2013 Framework for auditing ICFR will depend on the timing of the company's transition. We believe that in a manner consistent with the approach for disclosing the exact COSO framework used in management's ICFR assessment, it would be appropriate to indicate in the auditor's report the exact framework used.

Regardless of their decision, companies should clearly disclose in their annual assessment of ICFR whether they used the 1992 Framework or the 2013 Framework.

Implementation Challenges and Leading Practices

As companies work their way through the implementation process, some may resort to a checklist approach in complying with the new framework. To truly unlock the value that can be achieved by adopting the 2013 Framework, management should take a step back and evaluate how it is addressing the risks to its organization in light of the company's size, complexity, global reach, and risk profile. In companies' implementation of the 2013 Framework, there is a difference between doing the minimum to address the framework's principles and doing the *right thing* to effectively address the principles. Companies that choose to do the *right thing* will unlock the value, reduce fraud risk, avoid financial reporting surprises, and support sustained business performance over the long term.

The table below summarizes the 2013 Framework's principles by component, and the paragraphs that follow discuss common challenges that companies are experiencing as they work to implement the framework for SOX 404 purposes as well as leading internal control practices that may help address the implementation challenges.

Control Components and Summarized Principles				
Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities
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.	6. Specifies suitable objectives. 7. Identifies and analyzes risk. 8. Assesses fraud risk. 9. Identifies and analyzes significant change.	10. Selects and develops control activities. 11. Selects and develops general controls over technology. 12. Deploys through policies and procedures.	13. Uses relevant, quality information. 14. Communicates internally. 15. Communicates externally.	16. Conducts ongoing and/or separate evaluations. 17. Evaluates and communicates deficiencies.

[5] PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements.*

Demonstrating an Effective Ethics Program (Principles 1, 2)

As organizations evolve and change, their ethics programs may become stale or inadequate, and compliance with them may become "check the box" exercises. In addition, although many organizations have established ethics programs, they do not always address financial reporting or ICFR. Enron's code of conduct was widely acknowledged to be world-class at the time of the fraud scandal that ultimately ended the company and affected so many. In material fraud cases, there are often other alternate and conflicting messages in addition to those about integrity and ethical values. In many cases, the pressure on earnings and the personalities delivering alternate messages are so strong that they overpower the organization's message on integrity and ethical values. The tone that pervades such organizations can become a factor in employees' decisions to commit and rationalize fraud that they might not otherwise entertain. When it comes to tone at the top, actions speak louder than words.

When it comes to tone at the top, actions speak louder than words.

Common Implementation Challenges	Leading Internal Control Practices
As organizations evolve and change, their ethics programs may become stale or become "check the box" exercises. Further, although many organizations have established ethics programs, they do not always focus on integrating their financial reporting and ICFR expectations. Organizations often: • Lack a formal ongoing ethics program, including focused messaging on the importance of reliable financial reporting and ICFR. • Lack oversight of the ethics program by the audit committee. • Neglect to review the code of conduct for ongoing pertinence or update it in response to their changing environment, as needed. • Receive inadequate reinforcement by top and middle management or do not have ongoing training programs that specifically include financial reporting and ICFR. • Do not have relevant materials and resources readily available to employees or it is not in relevant languages. • Do not communicate expectations of integrity and ethical values to third parties and outsourced service providers. • Have inadequate ongoing training programs on ethics, including financial reporting. • Do not perform a periodic assessment of effectiveness. • Fail to sufficiently implement and closely monitor the ethics program in an acquisition. • Fail to sufficiently consider risks to effective ethics, including cultural, societal, or marketplace resistance to ethics and integrity (e.g., certain emerging markets in which bribes may be viewed as an acceptable business practice).	*Control environment:* • Management, under the direction and oversight of the audit committee, maintains an ongoing ethics program with an emphasis on reliable financial reporting and ICFR. • Management at all levels issues communications to reinforce the importance of a strong ethical culture, including topics related to financial reporting and ICFR. • The board of directors (audit committee) oversees the definition and creation of a code of conduct to establish standards and expectations concerning integrity and ethical values. • The code of conduct is provided to and acknowledged by new employees when they begin and annually thereafter. • The code of conduct is provided to and acknowledged by third parties. • The entity provides various protocols for reporting unethical behavior related to financial reporting and ICFR. • Unethical behavior related to financial reporting and ICFR is evaluated and resolved in a timely manner. • Management evaluates trends in the volume or nature of ethical behavior reported and determines whether to take steps to improve remediation actions regarding the ethics program. • Management performs periodic ethics assessments, including third-party ethics audits. • Violations of the code of conduct are addressed in a timely manner. *Information and communication:* • The entity's ethics program offers multiple channels through which unethical behavior by internal employees can be reported. • The entity's ethics program offers direct channels through which unethical behavior by external parties can be reported.

Risk Assessment, Including Performing an Effective Fraud Risk Assessment (Principles 7, 8)

Management's attention to risk assessment may be focused more on operational or regulatory risks than financial reporting risks; and in the context of financial reporting, it may be focused more on safeguarding assets and fraud, such as theft of inventory or fraudulent expense reporting (which generally represents only about 3 to 4 percent of the material frauds actually identified[6]), than on the risk of fraudulent financial reporting. Carefully identifying the entity's fraud risks, particularly when earnings pressures and aggressive incentive compensation programs exist, is an important part of a fraud risk assessment. In addition, management often does not adequately consider industry-specific risks and potential fraud schemes as part of the fraud risk assessment. For example, the potential for management override of internal control and financial reporting areas involving significant judgment and estimates should be specific areas of focus in a fraud risk assessment related to ICFR.

Because the risk assessment underpins the design and implementation of controls, an incomplete or ineffective risk-assessment process can have a significant effect on the effectiveness of ICFR. Further, significant errors or deficiencies (individually or in the aggregate) may indicate that the principles related to the risk-assessment component were not effective.

Carefully identifying the entity's fraud risks, particularly when earnings pressures and aggressive incentive compensation programs exist, is an important part of a fraud risk assessment.

Common Implementation Challenges	Leading Internal Control Practices
As organizations evolve and change, their risk-assessment process may become stale, and making updates, if they are made at all, may have become a "check the box" exercise. In addition, the entity's risk assessment may focus on operational or regulatory matters without adequately taking into account risks related to financial reporting and ICFR. In addition, with respect to fraud risk assessments, an entity may: • Not consider the relevant types of fraud when performing the assessment (i.e., fraudulent financial reporting, misappropriation of assets). • Not consider the ways that fraudulent financial reporting could occur, including: o Management bias (e.g., in the selection of accounting principles). o Degree of estimates and judgments in external reporting. o Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates. o Geographic regions where the entity does business. o Incentives that may motivate fraudulent behavior. o Nature of technology and management's ability to manipulate information. o Unusual or complex transactions subject to significant management influence. o Vulnerability to management override and potential schemes to circumvent existing control activities.	*Risk assessment:* • The entity reviews and updates its risk assessment annually: o The relevant risks for external reporting purposes are discussed, reviewed, and revised as necessary with input from the key functional and component managers. o Responses to each of the relevant risks are identified. • A fraud risk assessment is performed or updated annually to identify potential fraud schemes associated with external reporting, taking into account input from the key functional and component managers. • The results of the fraud risk assessment are discussed with the audit committee. *Control activities:* • The entity selects control activities that mitigate the risks identified in the risk assessment (also taking into account the fraud risk assessment), including control activities related to the IT environment.

[6] See Deloitte's *Ten Things About Financial Statement Fraud*.

Common Implementation Challenges	Leading Internal Control Practices
• Inappropriately consider residual risk as opposed to inherent risk. • Not reevaluate fraud risk periodically (e.g., annually) and as significant changes in the entity or its external environment occur. • Not consider risks with respect to the relevant activities performed by outsourced service providers. • Not review the results of the fraud risk assessment with the audit committee; or the audit committee may not effectively challenge management's assessment of fraud risks, including challenging the risk of management override of controls.	

Identifying Changes and Appropriately Factoring Them Into the Risk-Assessment Process (Principle 9)

Change creates risk; therefore, management should implement processes that enable it to identify and evaluate changes affecting the organization on a timely basis. While companies typically have robust change processes for IT systems, they often lack a defined process for managing other changes that could affect financial reporting, which may originate externally (e.g., new accounting requirements) or internally (e.g., accounting for nonroutine or complex transactions, business process redesign or centralization, or outsourcing to service providers). Sometimes the roles and responsibilities associated with these changes and the related controls are spread across multiple parties and are not effectively monitored. In addition, many companies underemphasize the importance of providing employee training on these new roles and responsibilities during the transition period, thereby creating a risk of ineffective internal control.

While companies typically have robust change processes for IT systems, they often lack a defined process for managing other changes that could affect financial reporting.

In practice, material weaknesses are frequently related to these changes and result in part from both an inadequate assessment of the related risks and insufficient deployment and monitoring of the controls that directly address the risks.

Common Implementation Challenges	Leading Internal Control Practices
• Lack of a detailed, thoughtful risk assessment involving the appropriate persons (and thus failure to identify and design appropriate controls). • Failure of management to properly assess the need for additional competency or to act on the need to involve others, including third parties. • Failure to consider and monitor changes in key personnel. • Unreliability of data used to evaluate or account for nonroutine transactions or events (e.g., data not subject to normal data quality controls may be inaccurate or incomplete). • Increased potential for management override (incentive or pressures may create bias). • Lack of consideration or objective evaluation of external events or trends and their impact on the entity's ICFR. • Lack of communication and coordination between functions (e.g., operations, tax, and financial reporting).	*Control environment:* • Lines of reporting and responsibilities affected by changes or events are evaluated and updated. • The entity monitors competencies related to external financial reporting and ICFR. *Risk assessment:* • Management (with input from functional or component management, third-party specialists, or both) determines whether a change or event gives rise to new or modified risks, including those related to fraud. *Control activities:* • In response to risks arising from changes or events, management determines whether (1) new controls are needed or (2) the risks are adequately addressed by existing controls (e.g., controls for identifying and evaluating complex or nonroutine contract terms). • Controls over the application of U.S. GAAP.

Common Implementation Challenges	Leading Internal Control Practices
	• Controls over the calculation of the impact of a change or event (including any IPE[7]). • System implementation change controls. • Internal control policies and procedures are updated to reflect the change or event, as applicable. *Information and communication:* • Information sources are identified, and communication channels are established, to facilitate timely identification of changes or events that may be relevant to ICFR. *Monitoring activities:* • Internal audit performs timely separate evaluations of control activities affected by new or nonroutine events or transactions. • SOX certification program requires confirmation that all relevant information has been provided.

Segregation of Duties (Principles 10, 11)

Many management teams and boards rightly worry about the risk that employees will collude to commit fraud. However, management's failure to segregate duties appropriately across multiple systems or manual processes poses the unique risk that employees will be able to commit fraud or conceal fraudulent activity without collusion. The opportunity to commit fraud and the likelihood of its occurrence are much greater when collusion is not necessary, as when duties are not appropriately segregated. This is particularly true in the era of large enterprise resource planning (ERP) systems, which individually process a substantial number of financial transactions. Detective controls alone, which may be imprecise and more operationally focused, are, by their nature, often ineffective in preventing or detecting fraud, especially since many material acts of fraud are not the result of a single material transaction and only become material in the aggregate over time.

Deficiencies in segregation of duties have been a common root cause of material weaknesses and material acts of fraud.

Deficiencies in segregation of duties have been a common root cause of material weaknesses and material acts of fraud. The following are a few examples of the numerous public-company internal control disclosures reported over the past 10 years about material weaknesses involving such deficiencies:

- "Specifically, the company identified deficiencies with respect to controls over segregation of duties, restricted access, changes to vendor and customer master data, transaction level and financial close which aggregated to a material weakness in internal control over financial reporting."
- "[There are] material weaknesses related to ineffective segregation of duties and general information technology controls to restrict user access and to review the development, change management, and maintenance of system applications."
- "[The failure to perform adequate user acceptance testing before implementing an ERP application] resulted in an inadequate segregation of duties and inadequate controls over approval of certain journal entries based on the roles assigned to users of the ERP."
- "[Material weaknesses identified in management's assessment include the] absence of proper segregation of duties within significant accounts and processes and ineffective controls over management oversight, including antifraud programs and controls."

[7] Information produced by the entity.

- "Material weaknesses in internal control over financial reporting [were] related to . . . lack of segregation of duties and weakness around timely and consistent management review of financial statements."

Common Implementation Challenges	Leading Internal Control Practices
• Duties may not be appropriately segregated across multiple systems or manual processes (e.g., access to both subledger and general ledger). • IT system access can give rise to significant or material issues because of an inability to control changes to system functionality or data (e.g., access to make and move a change). This can undermine the user's reliance on (1) automated system controls, (2) financial or control reports, and (3) the validity of source data for transactions in relevant systems. • Controls for ensuring the segregation of duties may not be adequately enforced globally, especially at smaller or more decentralized locations. • Mitigating controls (e.g., higher-level reviews of financial results) may not be sufficiently precise to mitigate the risk associated with segregation of duties.	*Control environment:* • Controls related to the audit committee's oversight of the risk of management override of controls. • Controls that assess and monitor the magnitude of the pressures on management to achieve targets. *Risk assessment:* • Controls related to the performance of an effective fraud risk assessment, which takes into account opportunities, rationalizations, and incentives or pressures to commit fraud. *Control activities:* • Controls that define and address the segregation of incompatible duties. • Controls that mitigate the risk associated with incompatible duties that may be incapable of being segregated. • Controls that identify IT controls for relevant systems that support ICFR, including: o Technology infrastructure controls. o Security management controls. o Technology acquisition, development, and maintenance controls. *Monitoring activities:* • Monitoring controls that periodically identify, evaluate, and remediate conflicts in user access that impede the segregation of duties. • Monitoring controls that periodically evaluate IT personnel access to systems related to ICFR.

Effective Design of Management Review Controls (Principles 10, 12, 13, 16)

Management's design of processes and controls typically consists of both preventive and detective controls (e.g., management review controls). However, management may be overrelying on such controls for SOX 404 purposes since they are often not precise enough on their own to detect material misstatements, particularly smaller or systemic errors that could aggregate into a material amount. Sometimes there is an operational bias in these controls (e.g., controls comparing actual to budget); while a control may identify a potential error when a variance occurs, it may not be designed to identify errors when a variance does not exist. For this reason, the design of management review controls and evidence of their operational effectiveness have been a significant area of focus for management, auditors, and regulators, particularly with respect to management review controls related to estimates and the application of U.S. GAAP to new or infrequent transactions or events.

When selecting controls to mitigate risks for ICFR purposes, management assesses the precision of a management review control by considering various factors.

Common Implementation Challenges	Leading Internal Control Practices
Management may overrely on a management review control that is not sufficiently precise, as in the following examples: • The purpose of the control is only to explain variances, not to assess whether the amounts recorded are appropriate. • Because performance standards and expectations were not clear, the control did not operate as intended. • The reviewer does not evaluate the underlying data or support at a sufficiently detailed or disaggregated level. • The reliability of the data (report) used in the control was not appropriately considered by the user. • The reviewer does not have a sufficient basis of knowledge and support to evaluate the data or identify errors. • The criteria for investigation used by the reviewer are too high, not well-defined, or not consistently followed. • The reviewer seldom asks questions or is not sufficiently diligent about following up to determine whether errors have occurred. • The evidence of conduct of the control is insufficient to enable the monitoring function to objectively determine what the reviewer considered and the basis for the reviewer's conclusions. • There is insufficient evidence of management's considerations under U.S. GAAP (e.g., the auditor's evaluation of U.S. GAAP takes into account matters not addressed by management).	*Control environment:* • All control owners, including management-level personnel responsible for management review controls, are held accountable for performance that falls short of expectations. *Control activities:* • When selecting controls to mitigate risks for ICFR purposes, management assesses the precision of a management review control by considering factors that include the following: o The purpose of the control. o The nature and significance of the risk that the control is designed to mitigate. o The level in the organization at which the control is performed (e.g., account balance, business unit/location, or the corporate level on a highly aggregated basis). o The nature of the data and reports used in the control, including the level of detail and support. o The reliability of the data and reports used in the control. o How frequently and consistently the control is performed. o The competency and knowledge necessary for the control owner to perform the control effectively. o The criteria and process used for investigation. o Whether the control is dependent on other controls, thus indicating that other, more precise controls should be identified. *Information and communication:* • Control policies and procedures are maintained and communicated on the entity's internal control intranet Web page. *Monitoring activities:* • Each quarter, control owners certify that they have performed the controls for which they are responsible in accordance with the established policies and procedures. • Internal audit periodically performs a review of the effectiveness of management review controls.

Outsourced Service Providers (Multiple Principles)

Given the significant increase in outsourcing relationships for information, business processes, and IT, internal controls related to outsourced service providers (OSPs) have become critical. While most companies have processes in place for evaluating SSAE 16[8] reports obtained from service organizations to address the control activities component of the 2013 Framework, most user organizations lack formal and auditable controls to address the OSP considerations related to the other four components of the framework

[8] AICPA Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization*.

(e.g., controls over the communication of expectations regarding the code of conduct, responsibilities, and authority; and controls for monitoring service-level agreements and communications). In addition, companies may directly record significant journal entries based on reports from OSPs without appropriate monitoring mechanisms to determine whether those reports are materially accurate and complete. It is important for management to establish robust monitoring controls over OSPs. Without such controls, there could be unfortunate surprises late in the year when SSAE 16 reports are delivered, such as unexpected report qualifications.

Common Implementation Challenges	Leading Internal Control Practices
• Expectations of integrity and ethical values not communicated to OSPs. • Lack of effective communication of the authority and approval policies; and inadequate monitoring of the roles delegated to others, including OSPs. • Failure to consider risks inherent in the relevant activities performed by OSPs, including fraud risks. • Failure to identify control activities performed by OSPs. • Failure to establish lines of communication with OSPs. • Failure to monitor control activities performed by OSPs.	*Control environment:* • Management and the board of directors consider OSPs when establishing organizational structures, reporting lines, and appropriate authorities and responsibilities. • OSPs are provided with clear and concise contractual terms related to the entity's expectations regarding conduct and performance, competence levels, expected information, scope of delegated authority, and communication flow. • Management evaluates the competence of OSPs. • Management evaluates the performance of OSPs against service-level agreements or other agreed-on standards. *Risk assessment:* • The risk-assessment process takes into account risks originating in OSPs, including possible acts of corruption by OSPs. • The entity updates its risk assessment for changes in the business, including relationships with OSPs. *Control activities:* • Management identifies (1) relevant controls at the OSP, (2) relevant controls within the entity, or (3) both. *Information and communication:* • Communication channels for reporting unethical behavior are made available to OSPs. • Information obtained from OSPs that manage business processes on behalf of the entity is subject to the same quality expectations as information generated by the entity internally. *Monitoring activities:* • The entity monitors the activities of the OSP, including obtaining and evaluating SSAE 16 reports as applicable (e.g., more frequent monitoring is performed for new OSP relationships until a stable state is reached).

It is important for management to establish robust monitoring controls over OSPs.

Information Quality (Principle 13)

Financial reporting misstatements may result from inappropriate reliance on erroneous data or reports, which could be triggered by failures in design or operational effectiveness related to any of the following:

- Controls over source data (i.e., manual or automated controls).
- Controls over interfaces and data transfers.

- Indirect general IT controls (GITCs) that support the reliability and integrity of system-generated information.

Sometimes, companies either lack appropriate controls for addressing the risks associated with important information on which they depend for SOX 404 purposes or fail to identify and test the controls over such information. A solution to this problem is ensuring that management has specific controls in place over data, including non-system-generated reports and data to and from OSPs. In addition, companies need to look beyond basic GITCs and also focus on the process-level controls over financial reporting information and data.

Sometimes, companies lack appropriate controls over data on which they depend for SOX 404 purposes.

Common Implementation Challenges	Leading Internal Control Practices
• The entity lacks a data governance strategy, policies, or standards defining control expectations for information. • The failure of information owners and users to design or implement controls over source data, report logic, or parameters compromises the information's reliability (i.e., completeness or accuracy). • Information requirements have not been updated to reflect the current state of the organization (e.g., change in business unit structure and system-generated reports). • Communication channels and controls for operational and regulatory information relevant to ICFR are ineffective. • Management has not appropriately considered controls over information from external parties (e.g., service organizations or management's experts) that are used in ICFR.	*Control activities:* • Various control activities are performed depending on the specific data and reports. For example: o Automated and/or manual controls are established to verify that transactional information (source data) is valid and accurate (e.g., vendor number and purchase order validation checks). o Management performs manual reconciliations of information between systems to validate the complete and accurate transfer of information between financial reporting systems. o GITCs over information security and program change control are designed and implemented for financial reporting applications and related infrastructure. o Spreadsheet controls are designed and implemented for all spreadsheets used for external financial reporting and ICFR. o Management implements controls over information transferred between the entity and external parties (e.g., service organizations, customers, and vendors). *Information and communication:* • Management establishes data governance strategies, policies, and standards for verifying the quality of information used in external financial reporting and ICFR. • Management supports the functioning of controls over data integrity through the maintenance of information, including flowcharts, data flow diagrams, process narratives, procedure manuals, and control procedures (e.g., controls over the preparation and maintenance of information used in controls). *Monitoring activities:* • Each quarter, control owners certify that they have complied with the established data governance policy and procedure. • Internal audit periodically performs tests in accordance with the established control policies and procedures.

Internal Control Design Evaluation (Multiple Principles)

If the design of entity-level controls is not fully evaluated, deficiencies in such controls may be overlooked. Given the requirement to separately determine whether each of the 17 principles in the 2013 Framework is present and functioning, entity-level controls are important foundational controls. In our experience, the majority of gaps are identified as a result of evaluating the design of controls and the ability of management, internal auditors, and external auditors to test those controls rather than as a result of performing a mapping exercise (i.e., mapping current controls to the 2013 Framework). It is important that management conduct a robust design evaluation to improve its internal controls and support its ICFR attestation.

Common Implementation Challenges	Leading Internal Control Practices
• Failure to properly evaluate the design of, and ability to test, entity-level controls.	• The following criteria are evaluated in the assessment of the design of an indirect entity-level control: o Detailed description of how the control is expected to be performed. o How the control addresses the related point(s) of focus and principle(s). o Authority and competence of control owner. o Frequency and consistency of operation of the control. o Considerations of the appropriateness of the criteria used for investigation (i.e., threshold) and the process for follow-up. o Dependencies on other controls or supporting data. • The following are questions considered and addressed related to the ability to test controls: o How will the operating effectiveness of the control be tested? o Can all attributes of the control be tested? o Is there sufficient, consistently available documentary evidence that the control is operating?

Use of the 2013 Framework for operational and compliance purposes (in addition to ICFR) is a growing trend among companies.

Using the 2013 Framework for Operational and Regulatory Compliance

Use of the 2013 Framework for operational and compliance purposes (in addition to ICFR) is a growing trend among companies. Implementing the updated framework provides a good opportunity, regardless of how mature a company's system of internal control may be, to take a fresh look at internal controls with the potential for creating value for the organization. Improvements in the effectiveness of a company's system of internal control can lead to more efficient operations, greater compliance rates, and more effective internal management reporting. Examples of voluntary uses of the 2013 Framework include the following:

- *Banking regulatory compliance* — While most banking and capital markets firms have used the COSO internal controls framework to design their SOX 404 ICFR compliance system, many are now taking a broader view of the updated framework. Many banking and capital markets firms are applying the principles of the COSO framework to design quality-assurance review functions over other areas, including operational and regulatory reporting. For more information about compliance trends in the financial services industry, see Deloitte's *In Focus: Compliance Trends Survey 2014*.

- *Cybersecurity* — Every organization faces a variety of cyber risks from external and internal sources. Cyber risks are evaluated against the possibility that an event will occur and adversely affect the achievement of the organization's objectives.

  Principle 6 in the 2013 Framework provides several points of focus that give organizations perspective on how to evaluate their objectives in a manner that could influence the cyber risk-assessment process.

  Because a cyber risk assessment informs decisions about control activities that are deployed against information systems and assets that support an entity's objectives, it is important that senior management and other critical stakeholders drive the risk-assessment process to identify what must be protected in alignment with the entity's objectives. For additional information, see Deloitte's *Changing the Game on Cyber Risk*.

- *Supply-chain risk management* — As a result of certain regulatory and operational risks such as food and product safety, conflict minerals, and consumer discontent with product performance, companies have increased their focus on proactively identifying and managing risks in the supply chain. Supply-chain risks are becoming board-level strategic risks for many companies. Accordingly, many companies are assessing their current risk exposure, implementing more formal governance structures, and designing more disciplined approaches to managing risks in the supply chain. These activities can help companies position their supply chain as a competitive advantage, manage regulatory risk, reduce or eliminate operational surprises, reduce the cost of doing business, and make informed capital allocation decisions. For more information, see Deloitte's *From Risk to Resilience: Using Analytics and Visualization to Reduce Supply Chain Vulnerability*.

- *Vendor management* — The application of the 2013 Framework to vendor management programs for OSPs to support their operations and compliance objectives (in addition to financial reporting objectives) can provide the necessary discipline to address an increasingly complex array of operational and compliance risks. Further, this discipline can enable organizations to control or reduce costs, mitigate risks, and drive service excellence. As a result, companies are using the 2013 Framework's concepts to establish new programs or enhance existing ones. Such enhancements include but are not limited to:

  - Ensuring that the OSPs understand management's commitment to integrity and ethical values.
  - Incorporating risks originating in the OSPs in the company's risk assessment process.
  - Developing monitoring procedures for key performance indicators related to service-level agreements as a means of identifying issues.

- *Change management* — Principle 9 of the 2013 Framework can broadly help a company effectively manage internal controls related to operational or regulatory changes. Companies may want to consider developing a process to apply Principle 9 and related concepts when major changes are identified to sustain and continuously improve internal controls related to operational or regulatory compliance.

Use of the 2013 Framework outside the financial reporting context can provide discipline to boards and audit committees as they address the increasingly complex array of risks they oversee.

Editor's Note: For additional examples of applying the 2013 Framework for operational and compliance purposes, see Deloitte's March 2014 *Audit Committee Brief*.

Use of the 2013 Framework outside the financial reporting context can provide helpful and necessary discipline to boards and audit committees as they address the increasingly complex array of risks they oversee. It can also provide management with a consistent and efficient framework to define, implement, and monitor its control structure and help it continually improve its overall risk management processes.

Subscriptions

If you wish to receive *Heads Up* and other accounting publications issued by Deloitte's Accounting Standards and Communications Group, please register at www.deloitte.com/us/subscriptions.

Dbriefs for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy and tax.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance, risk, and compliance.
- Technology.
- Transactions and business events.

Dbriefs also provides a convenient and flexible way to earn CPE credit — right at your desk. Subscribe to *Dbriefs* to receive notifications about future webcasts at www.deloitte.com/us/dbriefs.

Registration is available for this upcoming *Dbriefs* webcast. Use the link below to register:

- EITF Roundup: Highlights From the September Meeting (September 23, 2 p.m. (EDT)).

Technical Library and US GAAP Plus

Deloitte makes available, on a subscription basis, access to its online library of accounting and financial disclosure literature. Called Technical Library: The Deloitte Accounting Research Tool, the library includes material from the FASB, the EITF, the AICPA, the PCAOB, the IASB, and the SEC, in addition to Deloitte's own accounting and SEC manuals and other interpretive accounting and SEC guidance.

Updated every business day, Technical Library has an intuitive design and navigation system that, together with its powerful search features, enable users to quickly locate information anytime, from any computer. Technical Library subscribers also receive *Technically Speaking,* the weekly publication that highlights recent additions to the library. For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.

In addition, be sure to visit US GAAP Plus, our new free Web site that features accounting news, information, and publications with a U.S. GAAP focus. It contains articles on FASB activities and updates to the *FASB Accounting Standards Codification*™ as well as developments of other U.S. and international standard setters and regulators, such as the PCAOB, the AICPA, the SEC, the IASB, and the IFRS Interpretations Committee. Check it out today!