Deloitte.

Heads Up

June 10, 2013
Volume 20, Issue 17

In This Issue:

COSO Enhances Its *Internal Control — Integrated Framework*

by Jennifer Burns and Brent Simer, Deloitte LLP

On May 14, 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] released an updated version of its *Internal Control — Integrated Framework* (the "2013 Framework"). In addition, COSO released two illustrative documents, *Illustrative Tools for Assessing Effectiveness of a System of Internal Control* (the "Illustrative Tools") and *Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples* (the "ICEFR Compendium"), as well as an executive summary of the 2013 Framework.

Originally issued in 1992, COSO's *Internal Control — Integrated Framework* (the "1992 Framework") became one of the most widely accepted internal control frameworks in the world. COSO's primary objective in updating and enhancing the framework is to address the significant changes to business and operating environments that have taken place over the past 20 years.

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.

This *Heads Up* provides an overview of the enhancements in the 2013 Framework, a discussion of considerations for entities that use the 1992 Framework in complying with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), and information about making the transition from the 1992 Framework to the 2013 Framework, including impacts on other COSO-related documents. In addition, the appendixes to this *Heads Up* compare the 2013 Framework with the 1992 Framework as well as highlight some of the expanded concepts in the 2013 Framework. For additional information about the frameworks, see Deloitte's February 6, 2012, and August 7, 2012, *Heads Up* newsletters.

Enhancements in the 2013 Framework

The 2013 Framework creates a more formal structure for designing and evaluating the effectiveness of internal control by:

1. *Using principles to describe the components of internal control* — The 2013 Framework contains 17 principles that explain the concepts associated with the five components of the COSO Framework (control environment, risk assessment, control activities, information and communication, and monitoring activities). In developing the 17 principles, COSO focused on concepts from the 1992 Framework; considered the principles that were developed and articulated in COSO's 2006 *Internal Control Over Financial Reporting — Guidance for Smaller*

[1] COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership by developing frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. The five private-sector organizations are the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Management Accountants, and the Institute of Internal Auditors.

Public Companies ("Small Business Guidance"); and considered the significant changes in business, operating environments, and governance since 1992. COSO intends the principles to help companies design effective systems of internal control and evaluate whether those systems are functioning effectively. The 2013 Framework presumes that because the 17 principles are fundamental concepts of the five components, all 17 are relevant to all entities. Consequently, if a principle is not present and functioning, the associated component is not present and functioning. In rare circumstances, because of industry, regulatory, or operating matters, management may determine that a principle is not relevant to a component.

To further describe the principles, the 2013 Framework uses points of focus, which typically are important characteristics of the principles. While the points of focus may help management design, implement, and evaluate internal control and assess whether relevant principles are present and functioning, they are not required for assessing the effectiveness of internal control. Management may determine that some of the points of focus are not suitable or relevant and may identify and consider others.

2. *Creating a more formal way of designing and evaluating internal control in accordance with the principles.* See discussion below under "Effective Systems of Internal Control."

While the fundamental concepts in the 2013 Framework are similar to those in the 1992 Framework, the 2013 Framework adds or expands discussions about each component and principle.

While fundamental concepts in the 2013 Framework are similar to those in the 1992 Framework, the 2013 Framework adds or expands discussions about each component and principle, including enhancements such as the detailed points of focus. For example, although the concept of identifying and responding to risks was present in the 1992 Framework, the 2013 Framework includes more detailed discussions about risk assessment concepts, including those related to inherent risk, risk tolerance, how risks may be managed, and linkage between risk assessment and control activities.

In addition, unlike the 1992 Framework, the 2013 Framework explicitly includes the concept of considering the potential for fraud risk when assessing risks to the achievement of an organization's objectives (see Principle 8). The 2013 Framework explains that "[a]s part of the risk assessment process, the organization should identify the various ways that fraudulent [financial] reporting can occur, considering:

- Management bias, for instance in selecting accounting principles
- Degree of estimates and judgments in external reporting
- Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates
- Geographic regions where the entity does business
- Incentives that may motivate fraudulent behavior
- Nature of technology and management's ability to manipulate information
- Unusual or complex transactions subject to significant management influence
- Vulnerability to management override and potential schemes to circumvent existing control activities"

Principle 8 also discusses considerations relating to management override, safeguarding of assets, incentives and pressures, opportunities for inappropriate acts, as well as attitudes and rationalizations that may justify inappropriate actions. (See additional discussion of Principle 8 in Appendix A.)

Further, COSO has added considerations throughout the 2013 Framework regarding:

- Use of outsourced service providers (see Appendix B).
- Increased relevance of information technology (see Appendix C).

The table below summarizes the principles by component. Appendix A maps the principles to the topical sections in the 1992 Framework (as applicable) and summarizes, at a high level, some of the enhanced concepts in the 2013 Framework.

Control Components and 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 information. 14. Communicates internally. 15. Communicates externally.	16. Conducts ongoing and/or separate evaluations. 17. Evaluates and communicates deficiencies.

Each of the five components and relevant principles are required to be present and functioning.

Effective Systems of Internal Control

In an effective system of internal control under the 2013 Framework:

1. Each of the five components and relevant principles are required to be present and functioning. Under the 2013 Framework:
   - **Present** is defined as "the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives."
   - **Functioning** is defined as "the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives."
2. The five components are required to operate together in an integrated manner. The 2013 Framework explains that:
   - **Operating together** refers to "the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective."
   - Management can demonstrate that components operate together when:
     - The "components are present and functioning."
     - "Internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist."

Editor's Note: Under SEC rules related to compliance with Section 404 of SOX, "the assessment of a company's internal control over financial reporting must be based on procedures sufficient both to evaluate its design and to test its operating effectiveness."[2] Likewise, PCAOB Auditing Standard 5[3] requires the auditor to evaluate the design and operating effectiveness of the internal control over financial reporting. We believe "present" and "functioning" are equivalent to "design" and "operating effectiveness," respectively.

[2] Securities Act Release No. 33-8238, File Nos. S7-40-02 and S7-06-03 (August 14, 2003).
[3] PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements.*

The 2013 Framework uses the terms "internal control deficiency" and "major deficiency" to describe degrees of severity of internal control deficiencies. Under the 2013 Framework, an internal control deficiency refers to a "shortcoming in a component or components and relevant principle(s) that reduces the likelihood of an entity achieving its objectives," and a major deficiency refers to an "internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives." Further, the 2013 Framework explains that a major deficiency exists when "a component and one or more relevant principles are not present or functioning" or when "components are not operating together." In addition, if a major deficiency exists, the organization cannot conclude that it has met the requirements for an effective system of internal control.

Importantly, the 2013 Framework recognizes that in evaluating deficiencies in internal control, regulators, standard setters, and other parties may establish criteria for defining the severity of, evaluating, and reporting internal control deficiencies. To comply with internal control reporting requirements under SOX, management would continue to use the SEC's significant deficiency and material weakness terminology, and auditors would continue to use the same terminology under the PCAOB's standards. Accordingly, when a company is evaluating the design and operating effectiveness of its internal control over external financial reporting (ICEFR) (i.e., whether the principles are present and functioning) and identifies a deficiency, the company would be required to use the SEC's definitions and guidance to assess the severity of the deficiency, and the auditor would be required to use the definitions and guidance under PCAOB standards.

COSO has stated that it "will continue to make available its original Framework during the transition period extending to December 15, 2014, after which time COSO will consider it as superseded."

COSO Transition Guidance and Impact on Other COSO Documents

During the public comment process on the exposure draft of the 2013 Framework, various stakeholders requested that COSO provide a specific date for the transition from the 1992 Framework to the 2013 Framework to be completed. On the basis of this feedback, COSO has provided some transition specifics and is encouraging users to "transition their applications and related documentation to the updated *Framework* as soon as is feasible under their particular circumstances." COSO has also stated that it "will continue to make available its original Framework during the transition period extending to December 15, 2014, after which time COSO will consider it as superseded." In addition, SEC Chief Accountant Paul Beswick has stated that the "SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the future." He further stated that at this time, he "simply refer[s] users of the COSO framework to the statements COSO has made about their new framework and their thoughts about transition."

During the transition period (May 14, 2013, through December 15, 2014), COSO suggests that any "application of its *Internal Control — Integrated Framework* that involves external reporting should clearly disclose whether the original or 2013 version was utilized." As a result, when companies provide their annual assessment of ICEFR in accordance with SOX, it would be appropriate to indicate the exact COSO framework they used in performing the assessment.

Editor's Note: PCAOB Auditing Standard 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 ICEFR will depend on the timing of the company's transition. If the company uses the 1992 Framework for the calendar year ending December 31, 2013, the auditor would also use the 1992 Framework. We believe that in a manner consistent with the approach for disclosing the exact COSO framework used in management's ICEFR assessment, it would be appropriate to indicate in the auditor's report the exact framework used.

COSO's Small Business Guidance will be superseded by the ICEFR Compendium after December 15, 2014.

COSO's Enterprise Risk Management — Integrated Framework (the "ERM Framework") has not been superseded by the 2013 Framework. While the ERM Framework and the 2013 Framework are intended to have different focuses, the two frameworks are designed to complement one another. COSO believes that even though the ERM Framework includes portions of the text from the 1992 Framework, the ERM Framework continues to be suitable for designing, implementing, conducting, and assessing enterprise risk management.

COSO's Guidance on Monitoring Internal Control Systems, which was written to help organizations understand and apply monitoring activities in a system of internal control, also continues to remain relevant (i.e., it has not been superseded by the 2013 Framework). Appendix F of the 2013 Framework states that the "changes to the principles in the Framework will not substantially alter the approaches developed for COSO's Guidance on Monitoring Internal Control Systems."

Internal Control Over External Financial Reporting

The impact of the 2013 Framework on management's assessment of the effectiveness of ICEFR (i.e., to comply with SOX Section 404) will depend on how a company applied and interpreted the concepts in the 1992 Framework. For example, an existing system of internal control may not clearly demonstrate or document that all the relevant principles are present and functioning.

Companies should consider using 2013 activities, such as walkthroughs and tests of relevant controls, to identify necessary changes and field test application of the 2013 Framework.

COSO developed the ICEFR Compendium to help companies apply the 2013 Framework. The approaches discussed in the document describe how organizations may apply the principles in their system of ICEFR, and its examples illustrate the application of each principle.

Companies that use COSO to report on ICEFR may wish to consider:

1. Reading the 2013 Framework and identifying new concepts and changes.
2. Assessing their training and education needs.
3. Determining how the 2013 Framework affects the design and evaluation of ICEFR by:
    a. Assessing coverage of the principles by existing processes and related controls and considering the points of focus.
    b. Assessing current processes, activities, and available documentation related to applying the principles.
    c. Identifying any gaps in the above.
4. Identifying the steps, if any, to be performed in making the transition to the 2013 Framework, and:
    a. Formulating a plan to complete the transition by December 15, 2014 (i.e., calendar-year-end companies complying with SOX Section 404 should make the transition to the 2013 Framework for reporting periods ending after December 15, 2014).
    b. Considering using activities performed in 2013 (e.g., walkthroughs, testing of relevant controls, evaluation of deficiencies) to identify necessary changes and pilot or field test the application of the 2013 Framework.
    c. Confirming proper disclosure of the framework used during the transition period and at the time the 2013 Framework is adopted.
5. Coordinating and communicating internally with all groups that are responsible for implementing, monitoring, and reporting on the organization's ICEFR.
6. Discussing and coordinating activities with internal audit (if applicable) and the external auditor.

Illustrative Tools

COSO's Illustrative Tools provides examples of how a company may apply the 2013 Framework in assessing the effectiveness of its system of internal control. The document provides illustrative templates and includes scenarios with examples of how to complete various templates. However, the Illustrative Tools are not intended to:

- Satisfy any regulatory requirements for evaluating internal control deficiencies.
- Illustrate management's selection of controls to effect principles or address identified risks.
- Illustrate decisions about the nature, timing, or extent of testing of controls to ensure an effective system of internal control.

Appendix A — Comparison of Principles in the 2013 Framework With Related Sections in the 1992 Framework, and Summary of Enhanced Concepts in 2013 Framework

The table below maps the principles in the 2013 Framework to the topical sections in the 1992 Framework. The table demonstrates that, for the most part, the concepts represented in the principles in the 2013 Framework are similar to those in the 1992 Framework. However, the guidance that underpins the principles has been expanded, as indicated in the far right column, which summarizes at a high level some of the enhanced concepts in the 2013 Framework.

Principles in 2013 Framework	Related Sections in 1992 Framework		Summary of Enhanced Concepts in 2013 Framework
	Chapter	Section	
Control Environment			
1. The organization demonstrates a commitment to integrity and ethical values.	• Control Environment	• Integrity and ethical values • Human resource policies and procedures	• Integrity as a prerequisite to ethical behavior and an effective system of internal control. • Need to consider impacts of control environment across the structure. • Importance of: o Tone at the top as set by the board of directors and management. o Establishing standards of conduct for employees and outsourced service providers (OSPs). o Evaluating adherence to expected standards and addressing any deviations in a timely manner.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	• Control Environment	• Board of directors or audit committee	• Expanded discussion of governance concepts, including the need to establish oversight responsibilities for the board and its committees. • Matters related to board independence, skills, and expertise. • Includes a detailed table illustrating board oversight responsibilities for each of the five components of internal control.
	• Roles and Responsibilities	• Management, board of directors	
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	• Control Environment	• Management's philosophy and operating style • Organizational structure • Assignment of authority and responsibility	• Defining, assigning, and limiting authority and responsibility at different organizational levels and along the various lines of reporting (e.g., considering product or service lines, legal entity structures, geographic markets, and arrangements with OSPs).
	• Roles and Responsibilities	• Management, board of directors, internal auditors, other entity personnel	
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	• Control Environment	• Commitment to competence • Human resource policies and practices	• Planning and preparing for succession for those roles that are important to the effectiveness of internal control. • Expectation and evaluation of competencies. • Incorporates consideration of OSPs.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	• Control Environment	• Integrity and ethical values • Human resource policies and practices	• The importance of holding individuals accountable for their internal control responsibilities. • Aligning incentives and rewards with internal control responsibilities. • Considering excessive pressures. • Incorporates consideration of OSPs.
	• Roles and Responsibilities	• Management, board of directors, internal auditors, other entity personnel	

Principles in 2013 Framework	Related Sections in 1992 Framework		Summary of Enhanced Concepts in 2013 Framework
	Chapter	Section	
Risk Assessment			
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	• Risk Assessment	• Categories of objectives • Overlap of objectives • Linkage • Achievement of objectives	• Separates the financial reporting category into three objectives: (1) external financial reporting, (2) external nonfinancial reporting, and (3) internal reporting.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	• Risk Assessment	• Risk identification • Risk analysis	• Explains that the risk assessment process includes risk identification, analysis, and response. • Incorporates the concept of inherent risk. • Expands the discussion of risk tolerance and how risk may be managed, including by accepting, avoiding, reducing, and sharing risk. • Considers velocity and persistence of risk (in addition to impact and likelihood). • Incorporates consideration of OSPs.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	• Addendum to "Reporting to External Parties"	• Discussion[4]	• Incorporates the concept of fraud risk assessment. • Considerations related to various types of fraud, including fraudulent financial reporting, fraudulent nonfinancial reporting, misappropriation of assets, safeguarding of assets, management override, and corruption. • Evaluating incentives, pressures, opportunities, attitudes, and rationalizations. • Incorporates consideration of OSPs.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.	• Risk Assessment	• Circumstances demanding special attention • Mechanisms • Forward-looking	• Importance of assessing changes in the external environment, business model, operations, technology, relationship with OSPs, leadership, and how such changes may affect internal control.
Control Activities			
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	• Control Activities	• Types of control activities • Integration with risk assessment • Entity specific	• The linkage between risk assessment and control activities. • Consideration of the level at which control activities are applied (including various levels of the organization). • The types of controls applied (including considering preventive vs. detective controls). • Differentiates between business process control activities and transaction control activities.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.	• Control Activities	• Controls over information systems — general controls, application controls, relationship between general and application controls, evolving issues	• Incorporates updated technology concepts, including those related to technology infrastructure, security, acquisition, development, maintenance, and use of OSPs. • Discusses the relationship between automated control activities and general information technology controls.

[4] The addendum to "Reporting to External Parties" includes only a discussion of safeguarding of assets. Assessing the risk of fraud is not directly addressed in the 1992 Framework.

Principles in 2013 Framework	Related Sections in 1992 Framework		Summary of Enhanced Concepts in 2013 Framework
	Chapter	Section	
Control Activities			
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	• Control Activities	• Types of control activities — policies and procedures	• Establishing policies and procedures to support deployment of management's directives. • Establishing responsibility and accountability for executing policies and procedures. • Reassessing policies and procedures on a periodic basis to determine their continued relevance and if revisions are needed.
Information and Communication			
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	• Information and Communication	• Strategic and integrated systems • Information quality	• Identifying information requirements, verifying sources of data, processing relevant data, maintaining quality through processing, and using OSPs. • Considering the costs and benefits of information as well as the impact of technology. • Considering reliability and protection of data. • Reevaluating information needs. • Considering how information supports the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	• Information and Communication	• Communication — internal • Means of communication	• Importance of communication between management and the board of directors such that both have sufficient information to successfully fulfill their roles with respect to the entity's objectives. • Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines).
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.	• Information and Communication	• Communication — external • Means of communication	• Importance of open communication channels to allow input from stakeholders, including external party assessment results, to the board of directors. • Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines). • Considerations related to OSPs.
Monitoring Activities			
16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	• Monitoring	• Ongoing monitoring activities • Separate evaluations — scope and frequency, who evaluates, the evaluation process, methods, documentation, action plan	• Considering the rate of change when developing monitoring activities. • Using a baseline of understanding of internal control to establish plans for ongoing and separate evaluations. • Considerations related to monitoring at different levels of an organization and monitoring of OSPs. • Using technology in the context of monitoring.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	• Monitoring	• Reporting deficiencies — sources of information, what should be reported, to whom to report, reporting directives	• Communicating deficiencies. • Monitoring corrective actions.

Appendix B — Summary of Concepts and Discussion in the 2013 Framework Related to the Use of Outsourced Service Providers

The 2013 Framework adds or expands discussions about each component and principle by including enhancements such as the detailed points of focus. One of the significant additions to the 2013 Framework is the incorporation of considerations related to OSPs. The table below presents a summary of the 2013 Framework's concepts and discussions related to the use of OSPs. Users of the 2013 Framework should consider how these changes apply to their arrangements with OSPs.

Chapter in 2013 Framework	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Related to OSPs
Definition of Internal Control	N/A	4	• Acknowledges that management's operating model may use OSPs to support achievement of objectives.
Objectives, Components, and Principles	N/A	17	• A limitation of internal control is that third parties may circumvent controls through collusion.
Effective Internal Control	N/A	22	• Although the organization may rely on OSPs, management retains ultimate responsibility for meeting the requirements for an effective system of internal control.
Additional Considerations	N/A	24–25	• Dependency on OSPs changes the risks of business activities, increases the importance of information and communications from outside the organization, and creates challenges in overseeing activities and related controls.
Control Environment	Principle 1	33–38	• The organization's expectations related to integrity and ethical values are understood by OSPs. • The organization's standards of conduct are regularly communicated to OSPs and reinforced. • Inappropriate conduct by OSPs can reflect negatively on senior management and affect the entity itself by causing harm to customers, other stakeholders, or the reputation of the organization, requiring costly corrective action. • Management retains ultimate accountability for activities and performance of processes it delegates to OSPs. • The organization's standards of conduct provide the basis for evaluating adherence to integrity and ethical values by OSPs. • The organization communicates established tolerance levels to OSPs. • The organization defines a set of indicators to identify issues and trends related to the standards of conduct for OSPs. The organization also establishes compliance procedures.
	Principle 3	44–48	• Management and the board of directors consider OSPs when establishing organizational structures, reporting lines, and appropriate authorities and responsibilities. • Management ensures there is no conflict of interest in the organization and with its OSPs. • OSPs are provided with clear and concise contractual terms related to the entity's objectives and expectations of conduct and performance, compentence levels, expected information, and communication flow. • OSPs adhere to management's definition of the scope of delegated authority and responsibility as well as understand limitations of their decision-making rights.
	Principle 4	49–52	• The organization's commitment to competence, as communicated in policies and practices, facilitates measuring the achievement of objectives by OSPs. • Management evaluates the competence of OSPs relative to established policies and practices and then acts as necessary to address any shortcomings or excesses. • The organization's commitment to competence is supported by attracting, developing, evaluating, and retaining the right OSPs. • Management evaluates the performance of OSPs against service-level agreements or other agreed-upon standards. • Succession planning is undertaken by management when significant functions are delegated through contractual arrangements to OSPs.

Chapter in 2013 Framework	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Related to OSPs
Control Environment	Principle 5	53–58	• While OSPs may be used to carry out responsibilities together with or on behalf of the organization, management retains ultimate accountability for internal control. • Tone at the top helps to establish and enforce accountability, morale, and a common purpose, for instance by making upward and other communication channels available to OSPs for reporting violations of ethical standards. • Management and the board of directors consider the interrelationship between OSPs and performance measures, incentives, rewards, and pressures. • OSPs are expected to preserve the quality of products or services delivered, the safety of personnel, and other factors that could create a moral hazard or damage the organization's reputation.
Risk Assessment	Principle 7	70–71	• Risk identification must be comprehensive and take into account significant interactions between the organization and OSPs. • An organization's risk assessment process takes into account risks originating in OSPs.
	Principle 8	78–80	• The organization considers possible acts of corruption by OSPs during its fraud risk assessment, which should be based on the presumption that the entity's expected standards of ethical conduct are being adhered to. • In assessing possible corruption, the entity is not expected to directly manage the actions of OSP personnel; however, management may stipulate expected levels of performance and standards of conduct through contractual relations and may develop control activities that maintain oversight of OSPs.
	Principle 9	83–85	• Management assesses changes in relationships with OSPs to determine the relevancy of previously effective internal controls.
Control Activities	Principle 10	89	• When considering appropriate actions to mitigate risk, management assesses processes or functions performed in OSPs.
	Principle 11	98–100	• The organization's technology infrastructures may be outsourced to third-party service organizations and can present risks that management needs to understand and address. • The organization's technology development may be performed by OSPs. This represents unique risks and often requires selecting and developing additional controls over information submitted to and received by OSPs.
Information and Communication	Principle 13	109–112	• Management can generate useful information relevant to internal controls from data received from OSPs. • Information systems may be managed through relationships with OSPs. • Information that is obtained from OSPs that manage business processes on behalf of the entity is subject to the same internal control expectations (i.e., quality) as information generated internally by the organization.
	Principle 15	119–120	• An independent assessment of the internal controls at an OSP may give the organization important information about the function of its system of internal control. • The interdependence of business processes between the entity and OSPs can blur the lines of responsibility between the entity's internal control system and that of OSPs. • Communicating with OSPs responsible for activities supporting the entity's objectives may facilitate the risk assessment process, the oversight of business activities, decision making, and the identification of responsibility for internal control. • Complexities of business relationships between the entity and OSPs may arise. The entity should make separate communication channels available to OSPs to allow for direct communication with management and other personnel.
Monitoring Activities	Principle 16	132	• Entities that use OSPs need to understand the activities and controls associated with the OSP and how the OSP's internal control system affects the entity's system of internal control. Entities may gain an understanding of the OSP's internal control system by: o Conducting their own separate evaluations of the OSP's internal control system. o Reviewing an independent audit or examination report. o Considering the nature and scope of information transferred and the nature of processing and reporting.

Chapter in 2013 Framework	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Related to OSPs
Appendix B: Roles and Responsibilities	N/A	147	• When OSPs perform controls on behalf of the entity, management retains responsibility for those controls.
		149–150	• The CEO's responsibilities related to internal control include directing management and other personnel to consider the ever-increasing pace of change and networked interactions of OSPs and resulting risk factors. Senior management supports the CEO in this capacity.
		155	• While OSPs execute activities for or on behalf of the organization, management cannot abdicate its responsibility to manage the associated risks. Management must implement a program to evaluate activities performed by OSPs on its behalf to assess the effectiveness of the system of internal control.

Appendix C — Summary of Concepts and Discussion in the 2013 Framework Related to Information Technology

The 2013 Framework adds or expands discussions about each component and principle by including enhancements such as the detailed points of focus. In addition, the 2013 Framework reflects the significant changes in business and operating environments, including changes in information technology (IT), that have taken place since the 1992 Framework was written. One of the significant additions to the 2013 Framework is the expanded discussion of IT reflecting its increased relevance to organizations and their systems of internal control. The table below provides a summary of the 2013 Framework's concepts and discussions related to IT.

Chapter	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Related to IT
Objectives, Components, and Principles	N/A	6	• No two entities will, or should, have the same system of internal control; this is due, in part, to different degrees of reliance on IT.
Additional Considerations	N/A	24–26	• Specific controls are selected on the basis of management judgment and factors unique to each organization, such as its use and dependence on IT. • OSPs may perform IT activities that support business processes. Advances in IT have created cost-saving opportunities through access to comprehensive architecture providing on-demand and scalable shared technology that may otherwise be cost prohibitive for management to internally invest in. • IT may be essential to support management's pursuit of the entity's objectives and to better control the organization's activities. • The terms "technology," "management information systems," and "information technology" are used synonymously and share the ideas of using a combination of (1) automated and manual processes and (2) computer hardware, software, methods, and processes. • IT environments vary significantly in size, complexity, and extent of integration. • IT innovation creates both opportunities and risks. • The principles presented in the 2013 Framework do not change with the application of IT. Certainly, IT affects how an organization designs, implements, and conducts internal control.
		28	• Management considers a variety of cost factors related to expected benefits when selecting and developing internal controls, such as assessing the impacts of added reliance on IT.
Control Environment	Principle 2	39–43	• Management continually assesses risks posed by changes in the operating environment, such as emergence of new IT capabilities. • Composition of the board of directors is expected to include more specialized skills, such as those related to IT.
	Principle 3	44	• Management and the board use appropriate processes and technology to assign responsibility and to segregate duties.
		45	• Management is supported by requisite processes and technology to provide for clear accountability and information flows throughout the overall entity and its subunits.
		48	• IT is leveraged as appropriate to facilitate the definition and limitation of roles and responsibilities in the workflow of business processes.
	Principle 4	49	• The organization's policies and practices provide skills and conduct necessary to support internal control (e.g., knowledge of the operation of IT).
Risk Assessment	Principle 6	68	• Many organizations apply external IT standards to help manage their operations.
	Principle 7	72	• Risks at the entity level can arise from internal or external IT factors.
	Principle 8	79	• As part of its fraud risk assessment process, the organization should consider the nature of IT and management's ability to manipulate information.
		81	• The likelihood of a loss of assets or fraudulent external reporting increases when there are: o High turnover rates of IT staff. o Ineffective IT systems.
	Principle 9	85	• The organization identifies and assesses changes to IT to determine whether its system of internal control will need to be modified.

Chapter	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Related to IT
Control Activities	N/A	87	• Control activities are performed at all levels of the entity, at various stages in business processes, and over the IT environment.
	Principle 10	89	• When determining how to mitigate risk, management considers all aspects of the entity's internal control components and the relevant business processes, IT, and locations where control activities are needed.
		91	• Restricted access is important when IT is integral to an organization's processes or business.
		94	• Control activities and IT relate to each other in two ways: o IT supports business processes. o IT is used to automate control activities. • Most business processes have a mix of manual and automated controls, depending on the availability of IT in the entity.
	Principle 11	97–100	• The reliability of IT in business processes depends on the selection, development, and deployment of IT general control activities; important considerations include: o Understanding and determining the dependency and linkage between business processes, automated control activities, and IT general controls. o Selecting and developing control activities over the IT infrastructure. o Selecting and developing control activities that are designed and implemented to restrict IT access rights to authorized users. o Selecting and developing control activities over the acquisition, development, and maintenance of IT and its infrastructure.
	Principle 12	102–103	• Changes in IT may reduce the effectiveness of control activities or make some control activities redundant. Whenever change occurs, management should reassess the relevance of existing controls and refresh them when necessary.
Information and Communication	Principle 13	110	• Information systems encompass a combination of people, processes, data, and IT. • The nature and extent of information requirements, the complexity and volume of information, and the dependency on external parties affect the extent of IT deployed. • Information systems developed with integrated, IT-enabled processes provide opportunities to enhance the efficiency, speed, and accessibility of information to users. • IT solutions present opportunities for management to leverage IT in developing and implementing effective and efficient information systems.
		112	• Controls over retention of internal control information take into account the challenges of advances in IT, including communication and collaboration technologies used to support other components of internal control and achievement of the entity's objectives.
	Principle 14	116	• When choosing communication methods, management considers cultural, ethnic, and generational differences that can affect how messages are received (e.g., by using IT-based media).
	Principle 15	119	• IT enables external parties to have access to public forums to post and discuss an entity's business, activities, and controls. Controls are necessary to guide expectations for proper use to avoid jeopardizing the entity's objectives.
Monitoring Activities	Principle 16	128–129	• Companies frequently use IT to support ongoing evaluations. • Computerized continuous monitoring techniques have a high standard of objectivity and permit efficient review of large volumes of data at a low cost. Such techniques, combined with a robust review and analysis of results by knowledgeable personnel, result in efficient and effective monitoring.
Limitations of Internal Control	N/A	139	• Well-designed systems of internal control can break down when changes in IT application controls are implemented before personnel have been adequately trained.
Appendix A: Glossary	N/A	146	• The glossary includes the following definitions related to technology: o *Automated controls* — Control activities mostly or wholly performed through IT. o *Technology* — Software applications running on a computer, manufacturing controls systems, etc. o *Technology general controls* — Control activities that help ensure the continued, proper operation of IT. They include controls over the IT infrastructure, security management, and IT acquisition, development, and maintenance. They may also be referred to as "general computer controls" or "IT controls."

Chapter	Principle	Page(s)	Summary of Concepts and Discussion in 2013 Framework Relating to IT
Appendix C: Considerations for Smaller Entities	N/A	159–162	• Challenges for cost-effective internal control include controlling IT and maintaining appropriate general and application controls over computer information systems with limited technical resources. • Smaller entities often use software developed and maintained by others. Such software requires controlled implementation and operation, but many of the risks associated with systems developed in-house are reduced. • Commercially developed software packages can bring additional advantages to smaller entities, such as an embedded facility, related to controlling which employees can access or modify specified data.
Appendix E: Public Comment Letters	N/A	170	• The 2013 Framework does not extensively discuss specific IT initiatives or the risks associated with them because of the evolving nature of IT and concerns that the 2013 Framework would become dated.

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 & tax.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance and risk.
- Sustainability.
- Technology.
- Transactions & 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:

- Quarterly Accounting Roundup: An Update of Important Developments (June 27, 2 p.m. (EDT)).

Technical Library: The Deloitte Accounting Research Tool

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.

In addition, Technical Library subscribers have access to *Deloitte Accounting Journal* entries, which briefly summarize the newest developments in accounting standard setting.

For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.