COSO's Internal Control–Integrated Framework

Updating the Original Concepts for Today's Environment

By Jill D'Aquila

The *Internal Control–Integrated Framework*, issued by the Committee of Sponsoring Organizations (COSO) in 1992, was revolutionary: it represented the first major formal attempt to define internal control and provide a standard for measurement. Ten years later, the passage of the Sarbanes-Oxley Act (SOX)—specifically, section 404 of the act—further highlighted the importance of internal control. This law not only required organizations to establish and maintain internal controls over financial reporting; it also required managers and external auditors to evaluate and report on the effectiveness of internal control. The SEC also highlighted the importance of internal control shortly after SOX's enactment; in a final rule, the SEC stated, "The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements" (http://www.sec.gov/rules/final/33-8238.htm). The SEC recognized that other suitable evaluation standards existed outside the United States.

The PCAOB continued this focus on internal controls and, specifically, on the COSO framework in 2004, when it issued Auditing Standard (AS) 2, *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, and explicitly referenced the COSO framework as an appropriate framework to use when evaluating internal controls. Although the PCAOB issued AS 5, *An Audit of Internal Control Over Financial Reporting that Is Integrated with an Audit of Financial Statements*, in 2007 to supersede AS 2, the board continued to reference the use of a "recognized control framework" when auditors perform audits of internal control over financial reporting and when management evaluates the effectiveness of internal control over financial reporting.

Despite the existence of other available frameworks, the accounting profession recognizes COSO's *Internal Control–Integrated Framework* as a leading

framework for designing, implementing, and conducting internal controls and assessing their effectiveness. The majority of publicly traded companies in the United States rely on the framework. Globally, it has been widely accepted over the years and has been translated into seven languages; moreover, the core concepts of the framework still apply. Bill Schneider, director of accounting at AT&T and a member of the COSO Advisory Council, said in an AICPA webcast, "If you think about any document that has lasted 20 years without any revisions, that's pretty amazing" (http://www.aicpa.org/interestareas/frc/accountingfinancialreporting/pages/cosoupdatedinternalcontrolframework.aspx).

But this does not mean that the framework can, or should, remain unchanged. The following discussion explores the reasons behind the changes made in May 2013 to update the COSO framework for today's financial reporting environment.

Objectives and Integrated Components

COSO's *Internal Control–Integrated Framework* defines internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: 1) effectiveness and efficiency of operations 2) reliability of financial reporting 3) compliance with applicable laws and regulations" (http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf). These three objectives directly relate to five integrated components—control environment, risk assessment, control procedures, information and communication, and monitoring. The objectives identify what the organization wants to achieve, and the components identify what is required to achieve these objectives. The cube in *Exhibit 1* depicts the relationship between the three objectives and the five components; the third dimension in this cube is the structure of the organization.

No two organizations should have the same system of internal controls. Entities, objectives, and components should differ across different industries, sizes, and management models. COSO intentionally used a broad definition of internal control to accommodate a variety of organizations, industries, and geographic regions. Furthermore, the accounting profession views internal control as a dynamic process. According to the original framework's executive summary, internal control enables management to deal with a rapidly changing environment—but it is precisely this environment that produced the need to revise the original framework.

A Changing Business Environment

Although the core concepts of the framework have remained unchanged, the business environment is very different than it was 20 years ago. For example, consider how much technology has changed since the early 1990s. Organizations have become increasingly complex, as have the laws, rules, regulations, and standards that govern them. Markets and business operations are more global than ever before.

Another shift has occurred in the level of attention given to fraud prevention and detection. The passage of SOX is the likely cause. "Enron changed everything. … It raised the bar for law enforcement," according to Jordan Thomas, a former SEC lawyer, in a *Financial Times* article (Brooke Masters, "Enron's Fall Raised the Bar in Regulation," Dec. 1, 2011). Stakeholders are now more engaged and demand more accountability.

These changes have impacted all components of internal control, but other changes have targeted specific areas of internal control, such as monitoring. Naturally, there are greater expectations for governance and oversight. Monitoring functions, such as internal audit and corporate compliance, enjoy a higher status now. As a result, many asked whether the original framework sufficiently addressed this component.

Risk assessment is another specific area of internal control where additional guidance has been needed. Positions that simply did not exist in 1992, such as chief risk officer, have not only become commonplace but integral. In fact, the Institute of Internal Auditors (IIA) points out:

> In twenty-first century businesses, it's not uncommon to find diverse teams of internal auditors, enterprise risk management specialists, compliance officers, internal control specialists, quality inspectors, fraud investigators, and other risk and control professionals working together to help their organizations manage risk. ("The Three Lines of Defense in Effective Risk Management and Control," IIA Position Paper)

The IIA notes that each of these groups needs to have a clear understanding of its responsibilities and how it fits into an organization's internal control structure. But risk assessment and monitoring represent just two components of the framework. Given all the changes over the years, many have asked whether the original framework sufficiently addressed the control environment, control activities, and information and communication. In short, today's business environment has changed significantly since the early 1990s, leading COSO to update its framework.

COSO's Updated Framework

Much of the original framework remains intact: the updated *Internal Control–Integrated Framework* revolves around the same definition of internal control and requires the same five components for an effective system of internal control (http://www.coso.org/documents/coso%202013%20icfr%20executive_summary.pdf). In addition, it continues to emphasize the importance of management's judgment in designing and implementing, as well as assessing the effectiveness of, internal control. The updated framework simply "builds on what has been proven useful in the original version," according to COSO (http://www.coso.org/documents/COSO%20FAQs%20May%202013%20branded.pdf).

The updated framework does include enhancements and clarifications designed to guide users in applying it. Revisions to the original framework fall into three categories: 1) broad-based changes, 2) changes to the overall framework layout, and 3) changes to internal control components.

Broad-Based Changes to the Framework

The following changes cut across all areas of the framework.

Principles-based approach. The updated framework now contains 17 principles in order to more clearly explain the original framework's five components. These principles are broad because they are intended to apply to a wide variety of organizations, including publicly traded corporations, privately held companies, not-

for-profit organizations, and government entities.

Expanded reporting category. The updated framework expands the financial reporting objective to include other types of reporting, such as nonfinancial and internal reporting. Although financial reporting remains important, there is a growing interest in other types of reporting, including sustainability reporting and integrated reporting. The framework now recognizes this expanded view.

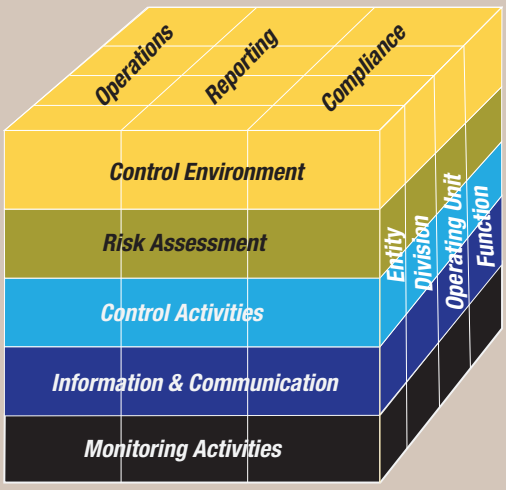
Other changes. The updated framework more fully discusses setting objectives related to internal control. It also features a discussion of governance, including the board of directors and its committees. Organizations are expanding outsourcing efforts as they look beyond their own walls for needed resources; they are also expanding globally. Accordingly, the updated framework recognizes both outsourcing and globalization by specifically referencing risk factors related to mergers and acquisitions and explicitly considering different business models and organizational structures.

The updated framework also recognizes that, as rules and regulations become more complex, the roles of regulators and standards become more central. As organizations become more complex, there are greater demands for accountability. COSO more fully discusses accountability in the updated framework. As the role of technology expands, the updated framework recognizes that these changes can impact how all components of internal control are implemented. Finally, there is considerably more discussion of fraud and antifraud expectations in the updated framework, as well as a fuller discussion of the relationship between fraud and internal control.

Overall Layout

The original framework contained one chapter that presented 1) the definition of internal control and the five components, 2) the relationship between objectives and components, and 3) effective internal control. The updated framework, on the other hand, organizes these topics into separate chapters. A separate chapter on effective internal control is easier to find and particularly helpful, according to the AICPA Internal Control Task Force, because it provides "a clear understanding of the requirements for an effective system of internal control" (http://www.coso.org/documents/IC_COSO_comments/8AICPA.pdf). A separate chapter contains additional considerations, including management judgment, cost versus benefits, technology, and organization size.

EXHIBIT 1
Objectives and Components of the Updated Framework



Source: Adapted from *Internal Control–Integrated Framework*: Executive Summary, http://www.coso.org/documents/coso%202013%20icfr%20executive_summary.pdf

Internal Control Components

The 17 principles are, perhaps, the most significant enhancement in the updated framework. They provide clarity regarding the role of principles in designing, implementing, and conducting internal control, as well as in assessing its effectiveness. These principles are specifically organized around each of the five components and, accordingly, have a significant bearing on the components; thus, if the relevant principle is not functioning, the presumption is that the component is not functioning appropriately.

Each principle is suitable to all organizations and all principles are considered relevant, unless an exception is specifically noted. In the AICPA webcast, Schneider described these principles as more overt: "You have to peel out what the principles are. … If you don't have these key principles, then you don't have a successful internal control structure." In the updated framework, COSO clearly describes the requirements for effective internal control. All components should be present and functioning, and internal controls across components should not result in one or more major deficiencies. A major deficiency represents an internal control deficiency or combination of deficiencies that severely reduce the likelihood of the organization achieving its objectives.

The new framework also includes points of focus, or important characteristics, of the principles. Points of focus might not be relevant to all organizations. In addition, organizations may identify other points of focus not stated in the updated framework. COSO indicates there is no requirement to separately assess whether points of focus are in place.

The 17 principles, organized around the five components, are discussed in the following sections. Each principle includes a discussion of the points of focus. A summary of similarities and differences between the original and updated frameworks follows each component, shown in *Exhibit 2*.

Control environment. The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the orga-

nization. The following five principles relate to this component.

Principle 1: "The organization demonstrates a commitment to integrity and ethical values." The actions of management and the board of directors should reinforce this commitment. Standards of conduct should define expectations concerning integrity and ethical values, and these expectations should be clearly understood. There should be processes in place to evaluate performance against expected standards of conduct. Any deviations should be identified and remedied in a timely fashion.

Principle 2: "The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control." Specifically, the board of directors should accept its oversight responsibilities and should define, maintain, and periodically evaluate the skills and expertise needed to enable the board to ask probing questions of senior management and take commensurate action. The board should be sufficiently objective and independent from management, and it should retain oversight responsibility for management's design, implementation, and conduct of internal control.

Principle 3: "Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives." Management and the board of directors should consider the multiple structures (e.g., operating units, legal entities, geographic distribution, outsourced service providers) to support the achievement of objectives. They should delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at various levels, including the board of directors, management, personnel, and outsourced service providers. Management should design and evaluate lines of reporting to facilitate the management of activities.

Principle 4: "The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives." Policies and practices should reflect an expectation of competence. The board of directors and management should evaluate competence across the organization and outsourced service providers. There should be mentoring and training to attract, develop, and retain sufficient and competent personnel and outsourced service providers. There should also be contingency plans for assigning responsibilities important for internal control.

Principle 5: "The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives." Management and the board of directors should establish the mechanisms to hold individuals accountable. They should also take corrective action as necessary. There should be appropriate performance measures, incentives, and other rewards that consider both short- and longer-term objectives. Incentives and rewards should be aligned with internal control responsibilities. Management and the board of directors should evaluate and adjust pressures as they assign responsibilities, develop performance measures, and evaluate performance. They should also evaluate the performance of internal control responsibilities and provide rewards or exercise disciplinary action as appropriate.

Overall comments. Interestingly, the control environment chapter of the original framework encompassed the same five principles. In addition, the roles and responsibilities chapter of the original framework discussed the second, third, and fifth principles. Nevertheless, the updated framework represents a significant change. It now explains the linkages between the different internal control components in order to highlight the central role of the control environment.

COSO more fully discusses a number of concepts incorporated in the control environment: Principle 1 provides numerous specific examples that indicate a lack of adherence to standards of conduct; Principle 2 contains a detailed discussion of board oversight and provides specific examples of oversight responsibilities, organized by internal control components. Furthermore, the updated framework provides guidance on determining board composition and specific capabilities expected of all board members, including general traits (e.g., leadership and critical thinking skills), as well as more specialized skills and expertise (e.g., market knowledge and financial expertise). Other principles more fully elaborate on integrity and ethical values to reflect lessons learned, different business models, and roles and responsibilities, as well as how they align with framework concepts.

Risk assessment. This involves a dynamic and iterative process to identify and analyze the risks of not achieving the entity's objectives, as well as forming a basis to determine how risks should be managed. The following principles relate to this component.

Principle 6: "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." These objectives relate to operations, reporting, and compliance.

Operations objectives reflect management's choices about structure, industry considerations, and the entity's performance. Management should consider some variation in achieving objectives and should include desired levels of financial performance. Management should use these operations objectives as a basis for allocating resources.

Reporting objectives encompass four types of reporting: 1) external financial reporting, 2) external nonfinancial reporting, 3) internal financial reporting, and 4) internal nonfinancial reporting. External financial reporting should comply with applicable accounting standards, reflect the underlying transactions, and show qualitative characteristics. Management should consider materiality when presenting financial statements. External nonfinancial reporting objectives should be consistent with the relevant criteria established by laws and regulations or recognized standards and frameworks. Internal reporting should reflect management's choices and should provide the information required to manage the entity. When preparing any reports, management should consider the required level of precision suitable for user needs. All types of reporting should reflect the underlying transactions and events.

Compliance objectives should reflect relevant laws and regulations. As with operations objectives, management should consider some variation in achieving these objectives.

Principle 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." The organization should consider both internal and external factors when identifying risks and should

implement risk assessment mechanisms at appropriate levels of management. Levels include the overall entity, subsidiary, division, operating unit, and functional levels. An important part of the risk assessment process involves estimating the potential significance of risk and considering how the risk should be managed. Risk management considers whether to accept, avoid, reduce, or share the risk.

Principle 8: "The organization considers the potential for fraud in assessing risks to the achievement of objectives." Types of fraud include fraudulent reporting, the loss of assets, and corruption. When assessing fraud risk, management should consider incentives and pressures, as well as the justification for inappropriate actions. Management should also consider opportunities for the unauthorized acquisition, use, or disposal of assets; the alteration of the entity's reporting records; and other inappropriate acts.

Principle 9: "The organization identifies and assesses changes that could significantly impact the system of internal control." These changes include the external environment, business model, and leadership. External environment factors include the regulatory, economic, and physical environment. The business model is characterized by new business lines, dramatically altered existing business lines, acquired or divested business operations, rapid growth, changing reliance on foreign geographies, and new technologies. Finally, leadership relates to management's attitude about internal control.

Overall comments. The original framework included an addendum to "Reporting to External Parties" that discussed safeguarding assets in connection with Principle 8. The risk assessment chapter of the original framework discussed the remaining three principles. The updated framework now specifically defines risk. Whereas the original framework did not directly address assessing fraud risk, Principle 8 now contains a detailed discussion on this topic. Inherent risk and fraud risk play a central role in risk assessment. The framework now contains a detailed discussion of the risk assessment process in Principle 7, which includes risk identification, risk analysis, and risk response. It also discusses risk tolerance and risk management, as well as the rate of change when determining the frequency of an organization's risk assessment process. Furthermore, Principle 6 separates financial reporting into the four separate categories described above.

Control activities. These are the actions established by an organization's policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of an entity, at various stages within business processes, and throughout the technology environment.

Principle 10: "The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels." Management should consider the impact of the environment, operations, and specific characteristics of the organization when selecting and developing control activities. Management should determine which relevant business processes require control activities and should implement control activities across various levels within the organization. There should be a mix of control activity types and a balance of approaches to mitigate risks. Control activities can be manual and automated, as well as preventive and detective. Control activities should include the segregation of incompatible duties or, if this is not feasible, alternative control activities.

Principle 11: "The organization selects and develops general control activities over technology to support the achievement of objectives." Management should determine the dependency and linkage between business processes, automated control activities, and technology general controls. Management should develop technology control activities designed to help ensure the completeness, accuracy, and availability of technology processing; to restrict access to authorized users commensurate with their job responsibilities in order to protect assets from external threats; and to provide control over acquiring, developing, and maintaining technology.

Principle 12: "The organization deploys control activities through policies that establish what is expected and procedures that put policies into action." These control activities should be built into the day-to-day activities of business processes through policies establishing expectations and relevant procedures specifying actions. Management should establish responsibility and accountability for control activities with management or the employees in the positions associated with the relevant risks. Control activities should be performed in a timely manner, and any necessary corrective actions should be taken. Employees performing control activities should be competent and have sufficient authority. Lastly, management should periodically review control activities to determine their continued relevance and should refresh them when necessary.

Overall comments. The control activities chapter of the original framework incorporated all three principles. The updated framework, however, modifies the description of control activities as 1) business process and 2) transaction control activities in Principle 10. It more fully discusses the relationship between control activities and risk assessment, control activities at different levels of an organization, preventive versus detective controls, and technology and related concepts. Overall, the updated framework provides a more detailed description of the types of control techniques and how to categorize them.

Information and communication. Information and communication are necessary for an entity to carry out internal control responsibilities in support of its objectives. Communication occurs both

Overall, the updated framework provides a more detailed description of the types of control techniques and how to categorize them.

internally and externally, and it provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance.

Principle 13: "The organization obtains or generates and uses relevant, quality information to support the functioning of internal control." The organization should be able to identify required information. Information systems should capture internal and external sources of data; process and transform relevant data into information; and produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information should be reviewed for relevance in supporting the internal control components. Lastly, the nature, quantity, and precision of the information communicated should be commensurate with the achievement of objectives.

Principle 14: "The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control." Such communication should include a process for the communication of required information; communication between management and the board of directors so that both have necessary information; and separate communication channels, such as whistleblower hotlines. These channels should serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective. Lastly, the timing, audience, and nature of the information should be considered when determining the method of communication.

Principle 15: "The organization communicates with external parties regarding matters affecting the functioning of internal control." External communication to parties such as shareholders, partners, owners, regulators, customers, and financial analysts should be both timely and relevant. Open communication channels should allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others. Relevant information should be communicated to the board of directors, and separate communication channels, such as whistleblower hotlines, should serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective. Lastly, the method of communication should consider the timing, audience, and nature of the communication, as well as legal, regulatory, and fiduciary requirements and expectations.

Overall comments. The information and communication chapter of the original framework incorporated all three principles. The updated framework, however, discusses the importance of the quality of information, as well as verifying sources and retaining such information. COSO expands the discussion of regulatory requirements, interaction with third parties, security and restricted access to information, costs and benefits of obtaining and managing information, and technological advances. Overall, the updated framework provides additional guidance on how information and communication support the other components of internal control.

Monitoring activities. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether all five components of internal control, including controls to effect the principles within each component, are present and functioning. These findings are evaluated and any deficiencies are communicated in a timely manner; serious matters are reported to senior management and the board.

Principle 16: "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." Management should consider the rate of change in business and business processes when selecting and developing ongoing and separate evaluations. Existing internal controls establish a baseline for ongoing and separate evaluations. Sufficiently knowledgeable individuals should perform these evaluations. Whereas ongoing evaluations are integrated with business processes, separate evaluations are varied in terms of scope and frequency, depending upon risk. These separate evaluations should be performed periodically in order to provide objective feedback.

Principle 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." The results of evaluations should be assessed and any deficiencies communicated to the parties responsible for taking corrective action, as well as to senior management and the board of directors, as appropriate. Lastly, management should track whether deficiencies are remediated on a timely basis.

Overall comments. The monitoring chapter of the original framework incorporated all three categories. The updated framework categorizes monitoring activities as ongoing and separate evaluations and discusses the need for a baseline to understand these types of evaluations. The new framework more fully discusses using technology and external service providers. In addition, COSO provides additional considerations regarding monitoring at different levels of an organization, as well as at third-party service providers.

The Principles and Professional Judgment

Although the 17 principles should help users in applying the updated framework,

it should be noted that the five components of internal control continue to be the focus of the requirements for effective internal control: each of the five components of internal control and relevant principles must be present and these five components should be operating together in an integrated manner (COSO's *Internal Control–Integrated Framework*, Framework and Appendices Chapter). Financial Executives International (FEI) believes that these 17 principles are helpful in applying

EXHIBIT 2
Fundamental Concept of the Framework Formalized as Principles

Control Environment	1. The organization demonstrates a commitment to integrity and ethical values. 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	6. The organization specifies objectives with sufficient clarify to enable the identification and assessment of risks relating to objectives. 7. The organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed. 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives. 9. The organization identifies and assesses changes that could significantly impact the system of 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. 11. The organization selects and develops general control activities over technology to support the achievement of objectives. 12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Information & Communication	13. The organization obtains or generates and uses relevant, quality information to support 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. 15. The organization communicates with external parties regarding matters affecting the functioning of internal control.
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. 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.

Source: Adapted from *Internal Control–Integrated Framework*. Executive Summary
http://www.coso.org/documents/coso%202013%20icfr%20executive_summary.pdf

the framework, but it cautions against using a checklist approach at the expense of professional judgment. "This project is not intended to change how internal control is defined, assessed, or managed, but rather provide more comprehensive and relevant conceptual guidance and practical examples," according to COSO chairman David Landsittel (http://pcaobus.org/News/Events/Documents/03242011_SAGMeeting/COSO_Briefing_Paper.pdf).

All in all, the updated framework is not designed to impose a higher threshold or additional burdens to achieve effective internal control; rather, "the principles and related points of focus will assist organizations in achieving their objectives, mitigating risk to acceptable levels, and adapting to changes in business, operating and regulatory environments," according to PricewaterhouseCoopers LLP ("COSO's Proposed Internal Control Compendium, Updated Framework, and Illustrative Tools," http://www.pwc.com/en_US/us/cfodirect/assets/pdf/dataline/dataline-2012-18-coso-compendium.pdf).

The AICPA Internal Control Task Force does believe that the updated framework will impose some additional burdens as organizations transition to it:

> Determining whether each of the 17 principles are present and functioning will require all preparers to undertake a "gap analysis," and reconcile their existing documentation and assessment processes to the updated Framework in order to ensure that the requirements are met. While the additional work necessary to bring documentation into alignment with the new Framework will vary from company to company, all companies will undoubtedly have some additional burden. (http://www.coso.org/-documents/IC_COSO_comments/8AICPA.pdf)

The AICPA Internal Control Task Force elaborates on this point:

> The Framework appropriately discusses the role and relevance of components, principles, and points of focus. … However, while the concept of the five components operating together in an integrated manner is not new, in practice the focus is primarily on whether they are present and functioning. Highlighting this requirement explicitly in the new Framework will prompt companies to consider the integrated functioning of their system of internal control in a more direct or systematic fashion. We think that many may find this to be challenging and it may take some time for companies to fully develop how they determine whether the components of their internal control system are truly operating together in an integrated manner. (http://www.coso.org/-documents/IC_COSO_comments/-8AICPA.pdf)

Transitioning to the Updated Framework

COSO presents the updated framework in three volumes: 1) the executive summary, which provides an overview for board of directors, CEOs, senior management, and regulators; 2) the framework and appendices that provide additional reference; and 3) illustrative tools for assessing effectiveness of a system of internal control (templates and scenarios to help apply the framework). COSO has concurrently published a "Compendium of Approaches and Examples" that contains practical illustrations of how the components and principles can be applied when preparing external financial statements (http://www.cpa2biz.com/AST/Main/-CPA2BIZ_Primary/InternalControls/-COSO/PRDOVR~PC-990026/-PC-990026.jsp).

COSO encourages users to transition to the updated framework as soon as feasible. Although COSO recommends that organizations promptly update their systems of internal control and related documents, it recognizes that each organization's particular circumstances will impact the time needed to do this. The updated framework will supersede the original framework on December 15, 2014. In addition, *Internal Control over External Financial Reporting* (ICEFR) will supersede the 2006 *Internal Control over Financial Reporting–Guidance for Smaller Public Companies*. During this transition period, organizations will need to identify whether they are using the original or updated framework for external reporting purposes.

Publicly traded organizations that are subject to SOX requirements, in particular, will need to pay close attention when reporting upon the effectiveness of internal control. These organizations should monitor guidance by regulators and standards setters for any preference regarding which framework to use during this transition period. The auditing literature, as well as attestation literature in general, will likely incorporate future changes based upon the updated framework. Although publicly held companies are the group most directly impacted by these changes, it is important to recognize that private organizations must also consider the AICPA rules that reference COSO for specialized engagements and representations of the effectiveness of internal control.

All in all, the updated framework is not designed to impose a higher threshold or additional burdens to achieve effective internal control.

The IIA points out that smaller organizations may face equally complex environments with a less formal, robust organizational structure when trying to ensure the effectiveness of their governance and risk management processes. Accordingly, a monitoring function, such as internal audit, might be equally important for a smaller organization. COSO offers specific considerations for smaller organizations in the appendices to the framework. In the end, all organizations—public, private, large, and small—will need to pay attention during the transition period. ❑

Jill D'Aquila, PhD, CPA, *is an associate professor of accounting in the Davis College of Business at Jacksonville University, Jacksonville, Fla.*