1

CHAPTER ONE

What We All Share

REGARDLESS OF THE type of entity, all Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework users and auditors in the public and nonpublic sectors share a great deal in common. We broadly outline those shared characteristics here before plunging into the details of application and documentation. This will also help readers to target the specific goals they have in studying this material. Later these concepts are developed in more detail. For now they serve to overview the subject matter.

NEED FOR CONTROL CRITERIA

Early auditing literature talked about controls, primarily in terms of controls over more routine transactions, such as cash receipts and disbursements. Based on the analysis of business and accounting failures over decades of experience, it became clear that a broader view of controls was necessary to address the various management, information processing, or oversight weaknesses that so often contributed to these events. However, there was no broader framework or set of criteria against which to evaluate the effectiveness of the entity in controlling its risk of filing materially false financial information and preventing other types of fraud. The COSO Framework has filled that void.

A set of criteria is a standard against which a judgment can be made. In the United States, the internal control integrated framework published by COSO is just about the only overall controls criteria to assess the effectiveness of internal controls over financial reporting (ICFR). Choosing an appropriate control criteria is a Securities and Exchange

Commission (SEC) requirement for public companies when performing an assessment of the effectiveness of an entity's internal control. The American Institute of Certified Public Accountants (AICPA) auditing literature references COSO components in its guidance to auditors of nonpublic companies, so from a practical perspective, COSO is the only game in town. While there are other frameworks out there (e.g., the criteria of control (COCO) framework from Canada, the Turnbull Report in the United Kingdom, and SOX of Japan), these are not that dissimilar to COSO in overall concept and have not gained wide acceptance outside of their home countries.

OVERVIEW OF THE COSO INTERNAL CONTROL INTEGRATED FRAMEWORK

In 1985, COSO was formed to sponsor the National Commission on Fraudulent Financial Reporting, whose charge was to study and report on the factors that can lead to fraudulent financial reporting. It was motivated by yet another intense period of time when financial reporting fraud and alleged audit failures were prominent in the news. Since this initial undertaking, COSO has expanded its mission to improving the quality of financial reporting. A significant part of this mission is aimed at developing guidance on internal control. In 1992, COSO published *Internal Control—Integrated Framework*, which established a framework for internal control and provided evaluation tools that businesses and other entities could use to evaluate their control systems.[1]

The COSO internal control framework identifies five components of internal control:

1. Control environment
2. Risk assessment
3. Control procedures
4. Information and communication
5. Monitoring

Today these remain unchanged from the 1992 Framework. That is a testament to the fundamental correctness of the COSO Framework. However, the level of detailed guidance over the years has increased due to the more recent widespread implementation of the Framework in our business environment and a desire to have more consistency in the application of COSO principles.

[1] In 2003, COSO published a draft of a document, entitled *Enterprise Risk Management (ERM) Framework*, whose purpose was to provide guidance on the process used by management to identify and manage risk across the enterprise. This new framework is not intended to supersede or otherwise amend its earlier internal control framework guidance on internal control. Internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding the discussion to form a more robust conceptualization of enterprise risk. *Internal Control–Integrated Framework* remains in place for entities and others looking at internal control over financial reporting by itself. Note: Entities using the *ERM Framework* will still need to make a pointed financial statement risk assessment, as detailed in the risk assessment component discussion.

HOLISTIC, INTEGRATED VIEW

The COSO Framework identifies five main components of internal control, and one of the keys of working with it is to understand how these components relate to and influence one another. COSO envisions these individual components as being tightly integrated in a nonlinear fashion. Each component has a relationship with and can influence the functioning of every other component, operating in an almost organic way.

The five interrelated components of the COSO Framework are, briefly:

1. *Control environment*. Senior management must set an appropriate tone at the top that positively influences the control consciousness of entity personnel. The control environment is the foundation for all other components of internal controls and provides discipline and structure.
2. *Risk assessment*. The entity must be aware of and deal with the financial reporting risks it faces. It must set objectives, integrated throughout its activities, so that the organization is operating in concert. Once these objectives are set, the entity is in a better position to identify the risks to achieving those objectives and to analyze and develop ways to manage them.
3. *Control activities*. Control policies and procedures must be established and executed to help ensure transactions being processed on a day-to-day basis, such as sales and expense transactions, or on a periodic basis, such as accruals and consolidations, are resulting in complete and accurate accounting recognition.
4. *Information and communication*. Surrounding the control activities are information and communication systems, including the accounting system. Whether manual or most likely today implemented using automated (computer) systems, they enable the entity's people to capture and exchange the information needed to conduct, manage, and control its operations. The information and communication component is comprised of both internal (e.g., management, governance) and external communications (e.g., shareholders, prospective investors, or creditors).
5. *Monitoring*. The COSO Framework identifies monitoring as the responsibility of management. The auditor is not a part of the entity's system of internal control. The entire company control process should be monitored on a regular basis by management, and issues that arise should be communicated appropriately within the organization. In this way, the system should be in a position to react dynamically, as changing as conditions warrant, and not require that special procedures or independent audit procedures detect these problems. The company is expected to be proactive in identifying and correcting control deficiencies.

Figure 1.1 is from the 1992 COSO *Integrated Framework* report. It depicts these five elements of internal control and their interrelationships in a 3-sided pyramid, with the control environment as the base.

Note that the information and communication component is positioned along the edge of the pyramid structure, indicating that this component has close linkages to the

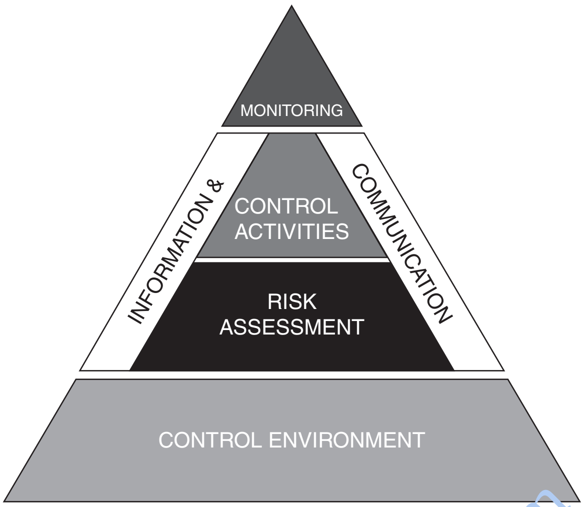

FIGURE 1.1 COSO Framework

other components. It probably would be even more accurate if the component were depicted as affecting all other ones, including control environment and monitoring, as it is difficult to envision these components being effective without effective information and communication.

Historically, the auditing literature has pictorially described the COSO Framework in the shape of a cube (see Figure 1.2). This representation shows that controls can

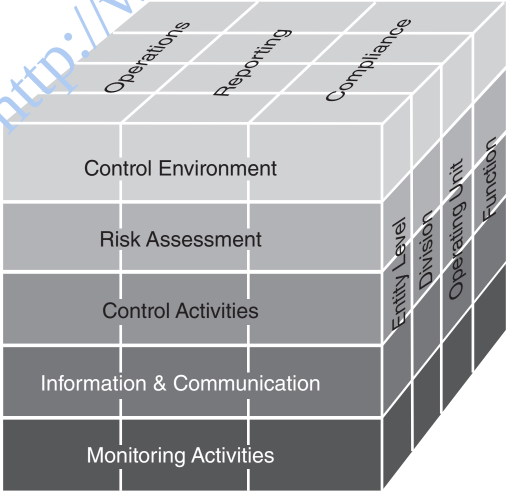

FIGURE 1.2 COSO Framework II

affect the entity either on an entity-wide basis or specifically on a divisional, regional or product line basis. The 2013 revision changed the "cube" and placed the control environment at the top of the cube. The strong hierarchical image of the pyramid and its strong base is somewhat lost in this representation, but for complex entities with multiple product lines or locations, the cube works well.

While both models have advantages, whatever the model used to communicate the Framework, it is helpful to have some physical representation of the Framework as a training tool and as a reminder of the components when initiating a project or bringing new personnel into an existing project. In the early days of Sarbanes-Oxley (SOX) implementation, some creative ways were developed to etch the components firmly in the auditor's mind. A unique product was a pen that revealed a new component each time the ballpoint pen point was retracted or extended.

A blessing of the COSO Framework is that together the five components seem to be satisfactory in describing the broad sources of internal control issues. The corresponding curse is that it is sometimes difficult to determine where specific facts and controls fall within the framework. While it would be nice if a one-to-one relationship existed between processes and controls and the Framework components, that is not the case. Entities can and did make their own decisions where controls belonged under the 1992 Framework. The focus and 17 Principles in the 2013 Framework will reduce the variability in classifying controls within the Framework going forward.

For example, the 1992 COSO Framework report contained only passing mention of information technology (IT). Can we clearly assign IT to just one component? Clearly there is a linkage to the control activities component since automated accounting processes and controls depend on the IT being effective. In another sense, IT is important to information and communication, which relies on data in company databases being accurate and complete. And it is hard to imagine running a business or performing the governance function effectively without accurate and timely financial data, so failures of IT can also impact the control environment. The fact is that IT has a pervasive effect on many aspects of the controls assessment and does not fit neatly into only one of the component categories. However, IT General Controls are now a specific principle to be satisfied (Principle 11).

Another example is fraud risk. There is now a principle (Principle 8) of risk assessment directed to assessing management's implementation of antifraud programs and controls. However, fraud risk can also be associated with the control environment, because of the risk of management override of controls. Fraud can be associated with transaction processing (a control activity) such as cash disbursements. So, prior to the recent guidance, it was not so clearly assigned to one component.

The point here is that while some topical issues fall neatly within a COSO component, there are control issues that may potentially affect many other components. That is also a reason that the new guidance stresses the interrelationship of controls and control deficiencies. One deficiency can touch several principles and components.

REVISED COSO INTERNAL CONTROLS FRAMEWORK

The revised COSO Framework (2013) replaces the 1992 and 2006 Framework guidance and documents. Those prior publications will be considered superseded after December 15, 2014. Some key elements of the new guidance include:

- Retention of the five basic components: control environment, risk assessment, control activities, information and communication, and monitoring.
- Identification of 17 Principles that are deemed essential to the five components
- Clear expectations that the elements of internal control work together in an integrated way.

Indeed, unless these elements are satisfied, COSO would conclude the system of internal controls is not effective.

Internal controls are defined in the revised Framework, and similarly in literature of the Public Company Accounting Oversight Board (PCAOB)[2] and AICPA, as: "a process, effected by the entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

This definition is consistent with the focus in the revised Framework on articulating the objectives in the three elements of operations, reporting, and compliance.

The COSO Framework retains these three elements of internal control. For purposes of this book, our focus is on the financial reporting element. However, as we discuss the issues surrounding this element, note that putting on blinders to issues from the other elements is not appropriate. Failures in operating controls can create increased allowances for returns and greater estimated warranty expenses, and failures in regulatory controls can cause liabilities for environmental issues or labor law violations with financial consequences. What may seem like a bright line in the diagrams is in reality a blurred line in practice.

In all cases, COSO and regulators expect the entity, and not the auditor, to be responsible for the design and implementation of the system of internal control. Likewise, all entities are expected to document and maintain updates to their internal processes and controls. In public companies, auditors are often impaired by independence rules from venturing very far into the design, assessment, and documentation process. In private companies, the auditor may be more helpful at present; however, future independence rules may limit auditor involvement in government and private engagements. Private companies should prepare to annually maintain and update the documentation of their controls systems. Auditors need to prepare their clients to do so.

Accompanying the Framework guidance are illustrative templates for documenting assessments, deficiencies, and aggregating issues from the detailed deficiency level to an overall conclusion. These templates may be structured as entities wish, but it

[2] For example, PCAOB Auditing Standard (AS) No. 5, paragraph A5.

may be worthwhile to note their suggested content in the development of proprietary approaches. Not published are forms, documents, and work programs to guide the entity or auditor when gathering information, performing assessments, and drawing conclusions. While various vendors may make such forms available to entities and auditors, the responsibility for ensuring the quality of those materials lies with the user, since COSO nor the auditing standards setters do not "certify" specific products.

The new guidance retains the much of the conceptual look and feel of the original 1992 Framework. In addition to guidance, there is a separate COSO volume with suggested approaches and examples of gathering evidence to support the principles, points of focus, and components. The COSO guidance should be accessible to the project leader or audit team, particularly in the initial period of implementation of the new guidance. In addition to purchasing the set of guidance at www.cpa2biz.com, various technical information vendors (e.g., Accounting Research Manager) have online versions for subscribers. Project leaders and audit team leaders should take the time to study these resources in some detail to ensure that the team is properly interpreting the principles and what sources of evidence might exist. Neither companies nor auditors are required to follow the suggested approaches or examples. They are presented simply as guidance; unlike the 17 Principles, they do not have to be satisfied or followed.

Although checklists are popular in auditing, users should resist creating checklists of controls in lieu of analyses, descriptions, and explanations of controls. COSO guidance seeks to ask the question "How do you accomplish this objective, or how do you satisfy this assertion?" and not whether a specific control exists or does not. In the identification of the points of focus articulated for each principle, it may be worthwhile to read these in connection with each principle and ensure that most are considered when assessing the effective implementation of the principle. While not a "checklist," the points are a helpful reminder of the scope of intended issues embodied in the principle. However, not all of these more than 80 points will apply to all entities.

Since 1992, business has changed in many ways. The 2013 Framework notably picks up two major trends and has implemented them widely in the new Framework. These trends include:

1. *Widespread use of outsourcing*. Today more and more business functions are being outsourced to third parties. Just because a function is outsourced does not remove it from the table when the function relates to ICFR. It should adhere to the same standards the entity is held to, including ethical standards of the entity. That includes outsourcing to far distant parts of the earth where cheaper wages may prevail. Outsourcing is mentioned in the discussions and examples of 12 of the 17 Principles. That does not preclude its application to other principles. Since 2003 the Securities and Exchange Commission (SEC) has required outsourcing entities to include a right-to-audit clause in agreements so that entities can ensure, if necessary, that controls are effective in the outsourced facility. Enhancements to the requirements for issuing Service Organization reports (e.g., Service Organization Control (SOC) Reports 1 and SOC 2) have also advanced the quality of these reports and their usefulness in placing reliance on outsourced functions.

2. *Widespread use of computer processing*. While the 1992 Framework gave limited mention of computer systems, the revised Framework weaves computer and network issues into the discussions of 14 of the 17 Principles.

Other changes brought about by the 2013 guidance will likely include:

- *More attention to areas other than control activities*. The 17 Principles and numerous points of focus will force many entities to gather more information than previously regarding the "softer" controls and assessments. It was perhaps easier for all to focus on transaction controls, but the new COSO guidance attempts to rebalance the efforts.
- *More focus on risk assessment*. Risk assessment is more carefully articulated, and more assessment is sought of the types of risk as well as the potential magnitude and likelihood of a risk occurring. In addition, the COSO introduces two new measures of the risk: *velocity* and *persistence*. Like a storm, the intensity of a risk and duration can have a very direct effect on the damage sustained. Hurricanes Sandy and Katrina and Midwest tornadoes provide evidence that some unlikely events can have devastating and long-lasting impacts. So also with some business risks. Risk assessment can be seen as a fundamental task that provides a framework for assessing the adequacy of the system of internal controls to prevent or detect material misstatement.

WHAT WE MUST DO

Entities should assess and document their internal controls. COSO and auditing standards agree that this is a responsibility of the entity. One often hears the concern voiced that entities have neither the expertise nor the manpower to perform this task. When such excuses are offered, the auditor often begins to question whether the lack of expertise might indicate a controls deficiency. An entity without the expertise to document controls might also lack the ability to design and monitor controls or to respond to issues that arise when controls fail. If the entity does not view internal control as a priority, then questions arise as to whether the control environment is lacking in some respect. The fact is that many entities would rather not bother with this responsibility, despite its overall value to society in adding integrity to investor reports and to the security and success of the entity itself. Attitude is important in shaping the quality of the controls and the quality of the oversight and continuous improvement that sustains and strengthens systems.

Entities and auditors should also have some evidence to support the fact that the descriptions of the internal controls relate to what is actually happening. That evidence may be through observation, examination of evidence, or reperformance of the control. Auditors are instructed to document their understanding of internal controls (and not the whole system of processes and activities). To the extent the entity has done the process and controls documentation well, the auditor can test that work and draw from it in lieu of reinventing the wheel.

All entities need to take a broad look at internal control over financial reporting (ICFR) and not ignore elements that are difficult to assess (the control environment, IT, or processes and controls that are outsourced). In some derivative applications of internal controls in other applications (SOX of Japan), only major processes are "in scope" for purposes of the assessment. There is no 80–20 rule or simple exclusions for U.S. generally accepted auditing standards (GAAS) applications. Materiality (alone or in aggregate) is the benchmark threshold for COSO assessments.

One message that rings clear in the 2013 COSO guidance is the need to articulate various management objectives in terms of operations, financial reporting, and regulatory compliance. These objectives are in turn the genesis for management to identify "risks" to their objectives. The risk assessment component in the Internal Controls Framework and in the COSO ERM relates risks to the stated objectives, answering the question: "Risks to what?" In reality, the objectives related to financial reporting might be fairly obvious. For example, "fair financial reporting in accordance with generally accepted accounting principles (GAAP)" would often be a high-level objective, and the presence of many estimates in the accounting process often presents risks to meeting that objective. An entity objective could also be to protect certain proprietary entity information from public disclosure and competitor scrutiny. The risks to that objective might be more meaningful to ponder and more specific to the entity. Entities should try to articulate their specific objectives, since meaningful risk assessments and the design and maintenance of controls to mitigate the risks follow from the objectives. While auditors may guess at the company-specific risks related to financial reporting and the assertions relating to financial reporting (completeness, existence, valuation, etc.) help structure the audit goals, auditors cannot possibly know all the nuances that management might be considering. Thus the assessment of risks associated with financial reporting is best performed by the entity and shared with the auditor. Too often it happens the other way around for many of the risks. Entities that fail to set objectives and identify risks are likely to exhibit and be assessed a material weakness in the risk assessment component of the Framework.

Transitioning to COSO 2013

Many entities will seek the quickest and easiest way to transition to COSO 2013. For many, there will be a significant number of additional control points to consider, since "2013" is more specific (using 17 Principles and numerous points of focus) than the original 1992 Framework. However, this challenge should also be viewed as an opportunity to reconsider any current documentation or approach and not to institutionalize past practices that may not be the most efficient and effective. The concept of "let's just get through this year" usually results in needed changes never being made and opportunities lost. While much of this book is devoted to providing the insight to assist in an effective and efficient assessment, there is a real issue of how to best take advantage of what has already been done and carry any best practices forward.

Those entities who adopted the 20 Principles outlined in the 2006 COSO guidance directed to smaller public entities will be farther down the road to converting to the 2013 guidance than those that by-passed this guidance and built their assessment process around the original Framework. As mentioned in the legacy versions of this work, that 2006 guidance was potentially useful to all entities and could be a real help in structuring effective assessment projects for any entity. And so it has come to pass. Where there was a change in the 2013 guidance from the 2006 version, this book also provides a road map of what has been added or reallocated to other principles. In addition, various hints are provided throughout the work to illustrate the potentially related principles when deficiencies are identified, in keeping with the integrated nature of controls as discussed in the 2013 guidance.

Mapping to the 2013 Guidance

One method used to map the 2013 guidance to the current project is to create a spreadsheet with the principles and relevant points of focus along one dimension and the previously identified controls along the other dimension. To be more effective, the matrix should also identify the relevant assertion(s) addressed by the controls (when assertions apply, such as for transaction controls) to ensure the coverage of the financial statements assertions and to identify any gaps. When identifying assertions, it may be appropriate to assign a numerical or letter value to the assertions you are using, so that the assertions covered can be sorted and gaps more easily identified. It may also be necessary to segregate the transaction- or disclosure-based controls by account or cycle so that the spreadsheet does not become unwieldy. Note that when considering cash controls, a deficiency might also indicate failure in a related principle, such as competence and training (Principle 4). It is a daunting task to pre-consider all the possible interactions between controls and principles and points of focus, so you may find some common linkages like the aforementioned example will be sufficient for mapping most controls. These linkages will not be automatic; they will depend on the specific root cause of the deficiency if it can be determined. A column or two could be allocated to identify potentially related principles. This task would be a new one, requiring familiarity with the 2013 approach and details of the principles and points of focus.

In total, the 2013 guidance notes 88 points of focus across the 17 Principles. However, a few of these points of focus are more closely related to operations and compliance objectives. Before discarding them from your analysis, note that such objectives often have a financial reporting implication in disclosure controls or for estimating allowance or reserve accounts. We discuss these issues further in connection with the risk assessment component itself.

Table 1.1 is an example template that maps identified entity controls to the 2013 guidance. You may wish to experiment with different approaches to this mapping before settling on one that makes the most sense for your organization, based on where you are and where you want to go. Depending on the component, subcomponent, and number of controls to be mapped, some matrices may be more effectively developed with the principles and points of focus across the top or down the side. While consistency in format is helpful, an unwieldy mapping format is not. Depending on the number of controls likely to be associated with a principle or related point of focus, it may be worthwhile to split the assessment into subsets (by component, by principles, or by other units, such as financial statement captions) that are more manageable. No one design will be perfect for all

TABLE 1.1 Mapping Controls to the 2013 COSO Framework

(a) Control Environment

Control ID	Primary Assertion	Secondary Assertion	P1 Ethical[3]	POF1	POF2	POF3 ...	P2 ...
CE1	NA	NA	X			X	
CE2	NA	NA	X	x			X

(b) Sales Cycle (P12)

Control ID	Primary Assertion	Secondary Assertion	Sales	POF1	POF2	POF3	POF4 ...
S 1	1	3	X			X	
S 2	3		X				X

entities and industries. The important thing is that all currently identified key controls are mapped and that all principles and points of focus are arrayed so that potential gaps can be identified.

While COSO clearly states that all the points of focus need not be met to be able to state that an effective system of ICFR exists, many are using the points of focus (and principles) to determine if there might be gaps in controls or yet-undocumented controls of importance that should be recognized. From a documentation standpoint, it is a short leap to expect that a point of focus (POF) considered irrelevant or not applicable will be supported with an explanation of why this is so.

A secondary benefit of this exercise is to assist the independent audit team in relating your assessment to their work paper tools and templates, which often are not customized to your entity approach. Auditors spend considerable time mapping entity approaches to audit requirements, time often better spent on more productive and useful activities or even reductions in seasonal workload.

BASIC SCOPING AND STRATEGIES FOR MAINTENANCE

All managements and auditors need to consider broadly the scope of ICFR. Just because a wide net is cast in examining controls does not mean that all of the controls under that net are key or critical; thus, testing and detailed analysis may not be required. However, managements were surprised in 2004 when controls over the hiring and use of specialists in determining fair values or allowances were declared by the PCAOB as in scope regarding ICFR. Current auditing standards require a specific assessment of the internal controls over the fair value estimation process. Nonpublic entity auditors are likewise directed by auditing standards to assess such controls over all estimates in the financial reporting process. Similarly managements and auditors were embarrassed when an academic, Professor Eric Lie, post-SOX, discovered that the values of stock options

[3] The notation P1 refers to Principle 1 and is noted this way throughout the text.

were being manipulated to benefit management in a number of large companies. This activity and process was not included in the early scoping of public company audits of internal control. A continuing conundrum is the issue of using service organizations for various accounting, IT, and data storage functions. A contemporary issue is the controls and security issue surrounding the use of cloud computing and cloud data storage. Outsourcing does not remove a function from the scope of internal controls assessment and analysis. Examples also exist of the failure to recognize the risks associated with trading or derivatives activities that may create exposures that exceed the apparent size of the operation; examples such as the Barings Bank collapse (currency trading) and Orange County, CA, bankruptcy (interest rate swaps) come quickly to mind.

The natural state of systems is for them to deteriorate over time. Managements, through monitoring and thoughtful annual reassessment, can keep a system in tune through an effective monitoring function. The absence or ineffectiveness of an effective monitoring function is likely to be a material weakness that would preclude an effective internal controls assertion or auditor reliance on controls to reduce other auditing procedures.

WHERE WE DEPART

Financial statement preparers of public, nonpublic, government, and nonprofit entities have the basic level of responsibility for assessing and documenting controls over financial reporting. While still responsible for the scoping, documentation, and verification that the described controls are implemented, nonpublic entities and their auditors may not need to test the controls as a basis for reliance on controls in setting the audit strategy. However, public companies have a specific requirement that they publicly assert the effectiveness of controls over financial reporting; doing that includes tests of the controls to be able to make that assertion. These various nonpublic entities and their auditors do have requirements that noted material weaknesses and/or significant deficiencies in controls (defined later) be reported to governance or to the overseeing regulator.

However, when auditors of any entity seeks to rely on the effectiveness of internal controls to reduce the scope of their other audit procedures, testing is necessary to confirm the assessment that the controls are designed and are operating effectively. Unlike in an attestation where high assurance is sought, the financial statement auditor may determine the right amount of testing and assurance to support the desired level of controls assurance from “low” (some) to “high.” When high assurance is sought, the project scope and testing level is similar to that required for an attestation. However, the assurance sought for controls reliance usually covers the entire audit period, not just the status of internal controls on the date of the report.

Nonpublic entities may optionally report on the effectiveness of their internal controls. Auditors can attest to these assertions under the revised AICPA attestation standards (e.g., AT 501). Alternative attestations allow for attestations on only the design of the controls or an attestation on both the design and operating effectiveness of the controls over financial reporting. For example, a nonprofit entity may wish to report on internal controls to provide assurance to donors of its stewardship over the donated funds and as a competitive tool to attract new donors. It seems likely that some government entities may soon be required to publicly report on their internal controls as a demonstration of their stewardship of public funds.

For certain regulated program audits (e.g., Office of Management and Budget [OMB] A-133 program audits of federal awards and programs), there may be specific audit requirements to meet compliance (with laws and regulations) that require tests of specifically identified controls over compliance by auditors. A source of confusion among some auditors is the fact that there exists very different guidance for financial statement and compliance-oriented government program audits. The focus of this book is on the ICFR.

Public companies report publicly on the effectiveness of their ICFR. As a result, SEC regulations require these entities to test controls as a basis for their assertion. There are specific exemptions from this requirement for companies when they first become public. Auditors of smaller public companies do not have to specifically report to the public on the effectiveness of the auditee's internal controls in the SEC 10-K annual filing. (This relief is now permanent under the Dodd-Frank Act of 2010.) However, auditors of larger public companies, accelerated filers,[4] *do* have to report to the public on the effectiveness of the auditee's internal controls in the required SEC 10-K annual filing. Therefore, auditors would also have a requirement to test internal controls as a basis for their assertion. The auditors of newly registered companies (under the Jumpstart Our Business Startups [JOBS] Act) may qualify for an exemption to auditor reporting on internal controls, provided revenues are under a predefined threshold.

As noted later, auditor oversight and testing may be important to ensure the quality of management's assertion regarding the effectiveness of controls. This seems to be particularly true as management first becomes familiar with controls issues.

TRIANGLE OF EFFICIENCY

Everyone desires an efficient project. From experience, an important consideration in achieving an efficient implementation of a controls assessment project is an understanding of the tasks and the acquisition of the skills before beginning in earnest the documentation, assessment, and testing process. Time and again the failure of one of the three key elements in what I call the triangle of efficiency (see Figure 1.3) is the root cause of wasted time and energy, and more often than not it results in an incomplete or incorrect assessment. This is an issue worth mentioning at the start, because false steps will cost money to correct.

The three knowledge components are:

1. Knowledge of entity and/or auditor requirements.
2. Knowledge of COSO.
3. Knowledge of company controls and processes.

[4] Accelerated filers have a market capitalization of $75 million or more.

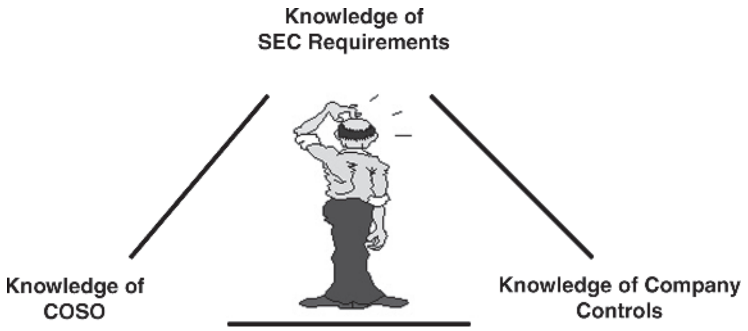

FIGURE 1.3 Triangle of Efficiency

In the case of public companies, their specific requirements are stated by the SEC. Private companies should look to COSO for guidance. While there is nothing contradictory about the SEC and COSO literatures, public companies should be familiar with the SEC-specific requirements, which may contain more detail regarding specific reporting and filing requirements. Public company auditors will be looking toward PCAOB Auditing Standard No. 5 for their requirements, which happen to be closely aligned with the SEC requirements, and ensuring public companies are following that guidance.

It often feels good just to get started on a project and begin to accumulate some evidence of progress. Indeed, that was a clear motivation in companies and auditors beginning to document the detailed activity-level controls over transactions before comprehending the scope of the requirements in 2004 when first reporting on controls under SOX. The resultant complaints about costs and time expended are intertwined with issues regarding failures to consider one or more of the three triangle components.

Experience says that if any of the three elements here is lacking, then there will be an impact on the efficiency and effectiveness of the overall project. Company consultants may be very competent in knowing COSO and knowing company and audit requirements, but they still have to learn the entity and its controls in order to perform their task. Close integration of company and consulting personnel can contribute greatly to efficiency of the company project over a strategy where the task is given primarily to the consultant. In the long run, the most efficient process is often one that is brought in-house and maintained by the entity. This controls focus in entity culture and auditing is not likely to go away. It is likely a part of our permanent business environment.

CONTROLS VERSUS PROCESSES

A good discussion to have before plunging into more subject matter here concerns the source of the surprisingly widespread misunderstanding regarding the distinction between controls and processes. COSO and the regulatory requirements for companies and auditors are directed at controls. The public company assertions about internal control effectiveness are directed at controls. So why is so much time and effort devoted to evaluating and documenting the business processes underlying the controls in company and auditor documentation? A significant potential source of efficiency and greater effectiveness in the controls documentation and assessment tasks is a clear distinction between controls and processes.

A simple example: A cash payment (cutting the check) is part of a process. A review of the support for the payment by someone other than the accountant is a control. A sale on credit initiates a process of shipment and recognition of a receivable. Checking the credit rating of the customer or checking that the customer is preapproved is a control over the validity or existence of the sale. The requirements are to document, assess, and test controls, not processes. But mountains of documentation are produced and retained in the name of controls documentation, which many times do not contain the description of a single real control.

If all the unnecessary documentation that has been produced magically evaporated from the hard drives and storage rooms of companies and auditors, some highly underutilized storage capacity would be revealed. Please understand, I know we are fond of our flowcharts, narratives that go on and on, and creating a lot of detailed descriptions of how things work. There is nothing wrong with all that. But the focus here is controls. How do we ensure completeness, how do we ensure our ownership of the assets we claim, how do we ensure the transactions are recorded in the proper period? As long as all these considerations (and a lot more to be discussed later) are addressed, the only drawback to the volumes we create are the updating review and edit we have to apply when changes occur and the mountains of data that has to be reviewed by management and the independent auditors. It's only money.

A current trend is away from the beloved narratives toward more flowcharting to document the business process and control points. However, it may be more efficient to keep separate controls documents than to muddy up flowcharts with all the data necessary to describe, assess, and hold the tests of the controls. Flowcharts or narratives can still be referenced to specific controls documentation.

By careful adherence to the spirit of the COSO Framework, the documentation of controls can be concise and organized. Whether you are just beginning in this process now or are seeking ways out of the quagmire of documentation produced previously, there is a way to meet the requirements without producing excessive volumes of documentation.

Internal Control Has Limitations

The existence of undesirable outcomes like misstatements and omitted disclosures may indicate that the process itself was flawed. However, that direct connection may not always hold true. It is possible that an internal control failure can be attributed to something other than a flawed process.

Internal control provides reasonable but not absolute assurance that an entity will achieve its financial reporting objectives. Even an effective internal control system can experience a failure due to:

- *Human error*. The people who implement internal controls may make simple errors or mistakes that can lead to control failures.

- *Management override*. Even in an otherwise well-controlled entity, managers may be able to override internal controls for selfish purposes.
- *Collusion*. Two or more individuals may collude to circumvent what otherwise would be effective controls.

Objective-Driven Approach

The COSO Framework views internal control as built-in to an entity's overall business processes, as opposed to a separate added-on component that attaches itself to the company's real business. Building in internal control requires that management do four things:

1. *Establish business objectives*. For our purposes, the most relevant objectives relate to financial reporting.
2. *Identify the risks to achieving those objectives*.
3. *Determine how to manage the identified risks*. The establishment of internal controls is just one of several options.
4. *Where appropriate, establish controls as a way to manage certain risks*. Individual controls are designed and implemented to meet the stated risks.

Internal controls have limited value by themselves—they do not produce a product or service or generate revenue for the business. Controls have value to the degree in which they help the entity to achieve its objectives through providing complete, accurate, relevant, and reliable information for decision making and for the fair communication of financial results to third parties. The effectiveness of internal control is judged according to how well it aligns with and addresses the objectives of the company.

Flexible, Adaptable, No One-Size-Fits-All Approach

The COSO Framework is a conceptual and not a rigid, prescriptive approach to internal controls. Thus, a paint-by-numbers approach is not going to be effective in complying with the aims of COSO. COSO recognizes that different entities will make different choices about how to implement controls in their businesses. The key is not whether the company uses control A or control B but whether the controls in place meet the risks by proper design and effective operation. COSO is not a checklist of suggested controls. Furthermore, management will make certain cost–benefit judgments and trade-offs. For example, an elaborate control structure over cash disbursements may be warranted in a large and complex business, but simpler controls may be effective and efficient in smaller enterprises. The result: Internal control is not a one-size-fits-all proposition, and a checklist of "usual" controls is not an effective tool to satisfy the COSO Framework guidance.

What can sometimes be frustrating about COSO controls guidance and the auditing standards is that simplifying the assessment and testing process through the use of practice aids is not easy. To have a successful project, it requires thought and understanding to apply the objectives of the Framework to a specific company circumstance. It takes knowledge of the entity and its processes, the regulatory environment, and the COSO Framework to make sense of the assessment and testing process. Early in the implementation of SOX, an experienced audit partner noted that she obtained a much better knowledge of her clients and their risks after going through the controls assessment process with them. Companies seeking practice aids to take the work out of the assessment process eventually realize this is not an achievable goal. However, an assessment and testing project done right is much easier to maintain over time than one cobbled together to get through this year. Think long term. Practice aids can still have value, but they must be adapted to the application. There is no turn-key approach out there, despite any Web site or brochure claims.

Furthermore, circumstances change at the entity, and so its internal control must be designed in a way to adapt and remain effective in a dynamic business environment. In fact, one of the primary objectives of the monitoring component of internal control is to assess the quality of the system's performance over time, recognizing that circumstances will change. In the 2013 guidance, analyzing and responding to change is a Principle (9) to be satisfied.

Reasonable Assurance

COSO recognizes the limitations of internal control. No matter how well designed or operated, internal control can provide only reasonable assurance that objectives will be met. Reasonable assurance is a *high* threshold, but it stops short of absolute assurance. The presence of an isolated internal control failure (less than a material weakness) does not, in and of itself, mean that a system is ineffective. The COSO even states that "even an effective internal control system can experience failure."

However, to be able to report publicly that internal controls are effective or to rely on the effectiveness of internal controls in lieu of other audit procedures requires that material weaknesses are either not present or are limited to specific areas that can be identified and mitigated by other procedures. When reporting on controls, the public expects a correspondingly high level of audit assurance.

People Factor

COSO recognizes that internal control is implemented by people. Documentation of controls is important, but documentation is not all there is to internal control. The effectiveness of internal control depends on the people responsible for carrying out individual control elements—from the chief executive officer and board of directors, all the way to rank-and-file employees charged with performing day-to-day transaction processing and control-related tasks.

Thus, the design of internal control must take into account the human element and must consider the role of human nature. For example, people are greatly influenced by the actions taken by an entity's senior management, more so than they are by what these individuals say. Therefore, the relative strength of an entity's control environment depends in large part on the actions of the entity's leaders and how they are perceived by the rest of the organization. This factor is assessed as part of the control environment.

The ability of individuals to carry out their responsibilities also depends on their competencies and how well they understand what is required. This need for understanding requires that the entity's internal controls have an effective hiring, training, and communication element. This is also an element of the control environment.

THE DEBATE CONTINUES

Companies and regulators continue to debate the cost–benefit of the requirements to assess and report on internal controls. Detractors have been somewhat successful in resisting auditor attestation in smaller public companies in the Dodd-Frank Act of 2010 and the JOBS Act of 2012. However, history has shown that inattention to internal controls is at the root of many business failures and frauds, which weaken investor confidence in the capital and stock markets. In addition, in the period before the imposition of the SOX Act of 2002, an alarming increase in the number of restatements of previously issued financial statements was observed. A lack of ICFR was a likely root cause of many of these restatements. A spike of fraud and restatement in smaller public companies may indeed bring reconsideration of the need for auditor verification of managements' assertions regarding controls.

It has been observed that certain categories of losses due to fraud and the incidence of restatements have come down in the post-SOX period. Whether this is due to greater management awareness of and attention to internal controls or strengthened auditor requirements regarding fraud and internal controls effectiveness is not known. What is clear is that there have been some notable improvements and reversals of downward trends, and thus the "medicine" seems to be working. The revised COSO Framework is intended to keep the ball rolling and help us to take the updates that have been issued since the original 1992 report and codify them into basic principles we can carry into the future.

Some executives have spoken out in favor of the value that the current regulatory requirements bring to the business environment. A recent survey of the Financial Executives Institute relates a more positive shift in management opinion when compared to the early days of the imposed regulations.

ORGANIZATION OF THIS BOOK

The remainder of this book will go into more depth on the 5 components and 17 Principles of the COSO framework and provide examples of the issues that arise in the assessment and testing of the controls. Specific reporting requirements of public companies are also covered throughout the book. Since many entities already are performing some controls assessments, the section on project management is placed farther back in this book than in previous editions; however, those new to this process (e.g., new companies, new personnel, and new responsibilities) or those seeking to improve current processes may want to review this material sooner or even next.

As the material is covered, there will be opportunities to speak directly to specific audiences, such as auditors or management or assessment team members, on specific issues, and these sections will be identified by special headings.

APPENDIX 1A

COSO 17 Principles

Component	Summary Principle
Control Environment	*1.* Demonstrates commitment to integrity and ethical values
	2. Exercises oversight responsibility
	3. Establishes structure, authority, and responsibility
	4. Demonstrates commitment to competence
	5. Enforces accountability
Risk Assessment	*6.* Specifies clear objectives
	7. Identifies and analyzes risk
	8. Assesses fraud risk
	9. Identifies and analyzes significant changes
Control Activities	*10.* Selects and develops control activities to mitigate risks
	11. Selects and develops information technology general controls
	12. Deploys controls through policies and procedures
Information and Communication	*13.* Uses relevant information
	14. Communicates internally
	15. Communicates externally
Monitoring	*16.* Conducts ongoing and/or separate evaluations
	17. Evaluates and communicates deficiencies