The Committee of Sponsoring Organizations of the Treadway Commission

Internal Control – Integrated Framework

Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting

Executive Summary

Guidance

For Public Comment

Please provide comments to www.ic.coso.org

before December 31, 2005

October 2005

Committee of Sponsoring Organizations of the Treadway Commission

Board Members	Representative
COSO Chair	Larry E. Rittenberg
American Accounting Association	Mark Beasley
American Institute of Certified Public Accountants	Charles E. Landes
Financial Executives International	Nick Cyprus
Institute of Management Accountants	Dennis L. Neider
The Institute of Internal Auditors	David A. Richards

PricewaterhouseCoopers LLP

Principal Contributors

Miles Everson
Project Leader
Partner
New York City

Mark Cohen
Senior Manager
Boston

Chris Paul
Senior Associate
Boston

Frank Frabizzio
Partner
Philadelphia

Erinn Hansen
Senior Manager
Philadelphia

Mario Patone
Manager
Philadelphia

Tom Hyland
Partner
New York City

Frank Martens
Director
Vancouver, Canada

Shurjo Sen
Manager
New York City

Paul Tarwater
Partner
Dallas

Observer

Jennifer Burns
Professional Accounting Fellow
Securities and Exchange Commission

Project Task Force to COSO

Guidance

Deborah Lambert
Chair
Partner
Johnson, Lambert & Co.

Joseph Carcello
Professor of Accounting
University of Tennessee

Douglas F. Prawitt
Professor of Accounting
Brigham Young University

Christine Bellino
Jefferson Wells International, Inc.

Rudolph J.J. McCue
WHPH, Inc.

Malcolm Schwartz
CRS Associates LLC

Members at Large

Carolyn V. Aver
CFO
Agile Software Corporation

Gus Hernandez
Partner
Deloitte & Touche

Pamela S. Prior
Director of Internal Control & Analysis
Tasty Baking Company

Kristine M. Brands
Senior Analyst
Oracle Corporation

Andrew J. Jackson
Senior Vice President of Enterprise Risk Assurance Services
American Express Company

James K. Smith, III
Vice President & CFO
Phonon Corp

Thomas M. Berger
Management Resources Division
Robert Half International

Brian O'Malley
Chief Audit Executive
Nasdaq

Dan Swanson
Director Professional Practices
The Institute of Internal Auditors

Serena Dávila
Director for Private Companies & Small Business
Financial Executives International

Andrew Pinnero
JLC/Veris Consulting LLC

Kenneth W. Witt
American Institute of Certified Public Accountants

Table of Contents

The Committee of Sponsoring Organizations of the Treadway Commission

Internal Control – Integrated Framework

Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting

Executive Summary

EXECUTIVE SUMMARY

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework* (the *Framework*) to help businesses and other entities assess and enhance their internal control systems. Since that time, the *Framework* has been recognized by regulatory standard setters and others as a comprehensive framework for evaluating internal control, including internal control over financial reporting.

Many changes have taken place in the financial reporting, corporate governance, and regulatory environment since the *Framework* was issued. Most significantly, the Sarbanes-Oxley Act of 2002 (the Act) was passed by the United States Congress and signed into law by the President on July 30, 2002. Among other provisions, Section 404 of the Act requires management to annually assess and report on the effectiveness of internal control over financial reporting. COSO recognizes that Section 404 of the Act is a major driver of a company's evaluation of internal control over financial reporting. Yet, even in light of this development, the concepts first set out in the *Framework* remain appropriate today. This document is not intended to reduce or limit application of the principles set out therein.

The objective of this document is to provide guidance for smaller public companies and their auditors to assist them in applying the *Framework* in connection with assessing and reporting on the effectiveness of internal control over financial reporting. Secondarily, it illustrates ways to design and implement effective internal control in a cost-effective manner.

Key Considerations Addressed in This Guidance

The *Framework* is based on fundamentally sound control principles that are applied daily in all organizations. This guidance summarizes twenty-six fundamental principles that constitute effective internal control over financial reporting. These principles are equally applicable to both larger and smaller businesses, governmental agencies, and not-for-profit organizations. Smaller companies, however, are different from their larger counterparts and may implement effective internal control in a different manner. Management of smaller companies tends to have a hands-on approach, wider spans of control, and the ability to provide ongoing monitoring through direct relationships with key personnel, vendors, customers, and capital providers. Management's hands-on approach in smaller businesses can create opportunities whereby controls may be less formal without decreasing their quality.

A common burden for smaller companies is evidencing that controls are working effectively. When management of smaller organizations relies on internal controls solely for running the business and makes no public assertions on effectiveness, the level of

controls and documentation is often less formal, due in part to greater concentrations of decision-making authority, wider spans of control, and more direct channels of communication.

When management asserts to a third party on the design and operating effectiveness of internal control, there usually is a need for greater formalization in the control processes and a certain level of documentation to provide evidence the controls are working effectively. Further, some controls must be more formalized to ensure that transactions are processed correctly and consistently.

There is a cost to additional formalization and documentation. However, for most companies, there can be important benefits associated with additional documentation, such as:

- More efficient and effective financial reporting
- Better data for decision making
- Increased investor confidence, which can reduce the discount rate for pricing investment securities
- Access to public capital markets.

COSO recognizes that applying the *Framework* can and should differ for smaller businesses and has identified several themes for specific attention by smaller businesses:

- The ***control environment*** is very important and sets the tone for internal control in a company. In smaller businesses, the actions of management and its demonstrated commitment to effective governance and control are often more transparent.
- In determining what controls are necessary, a company should consider ***risks*** to reliable financial reporting and then identify controls required to mitigate those risks, rather than focusing solely on mandating specific control. The focus should be on controls that mitigate risks related to financial statement assertions and account balances.
- ***Control activities*** require a minimal level of formalization. This is necessary so that everyone understands their responsibilities, how the controls operate, and the importance of the control process.
- ***Information technology*** can be an enabler of effective internal control. While information technology often has been cited as a source of control risk, smaller businesses can take advantage of information technology to promote more effective control.
- ***Monitoring*** the effectiveness of internal control can take place in many different forms in smaller companies. This includes ongoing monitoring that is already in place, including monitoring by executives who have direct and explicit knowledge of the

activities of the business. These controls often are relied on by management in smaller companies.

- Employees can and should understand objectives related to financial reporting, risks, and their ***personal responsibility for controls.*** Even smaller companies can implement effective procedures so that when employees note control problems or deviations from acceptable practices, they can report these findings to the right place before they become a significant issue for the company.

The themes noted above have influenced the approaches articulated in the remainder of this document.

Controls Need to Be Cost Effective for Smaller Businesses

Although it is often difficult to measure the risks associated with inaccurate financial reporting, market reactions to corporate misstatements clearly signal that the market does not readily tolerate inaccurate reporting, regardless of a company's size. Accordingly, an effective internal control system can add value to a company. However, a company, and particularly a smaller company, may incur additional costs to design effective controls over financial reporting and demonstrate they are in place. A company can lessen the amount of those incremental costs and still maintain appropriate levels of internal control by implementing the principles contained in this report. Internal control should be established and maintained in a way that meets the objectives of reliable financial reporting in a cost-effective manner.

There are many options available for smaller businesses to reduce the costs of internal control. We have identified several that are summarized below and discussed further throughout this document.

- *Broaden the Pool of Audit Committee Members* – Audit committees can provide valuable insight and oversight, helping companies apply internal control in a cost effective manner. The population from which potential board and audit committee members are selected, can be expanded by considering highly qualified individuals with financial expertise. Some options include:
  - Chief financial officers
  - Management accounting experts
  - Accounting professors with detailed knowledge of business, accounting, and auditing
  - Chief audit executives (internal audit directors) who have experience in internal control and business strategy from their own businesses
  - Retired partners from public accounting firms.
- *Build Controls into the Culture* – Building control responsibility and control knowledge into the culture is often the most effective way to reduce costs.

- *Sharpen the Risk Focus* –The internal control process should be focused on areas that represent significant risks to the achievement of reliable financial reporting.
- *Use Software Templates for Design and Evaluation* – Templates or readily available software tools can facilitate the design and evaluation of controls.
- *Use Information Technology to Standardize Controls* – Information technology (accounting software) can be used to (a) implement consistent controls, and (b) enhance segregation of duties.
- *Leverage Management Monitoring* – With its knowledge of the company, management can provide effective monitoring of the financial reporting process.
- *Outsource Some Activities* – It may be possible to outsource some activities, including parts of monitoring or internal audit.
- *Organize Evaluation Around Principles* – Exhibit 1.1, along with the chapter overviews, can be used as a checklist of principles to consider in developing effective internal control over financial reporting.

Further, the guidance includes in each chapter a discussion of alternative approaches and provides detailed examples taken from smaller companies. For instance, the guidance illustrates how a less formal, but still effective, ethics program might include posting of a statement of values in all work places, how reliance on information technology controls can be improved when using packaged software applications, and how approaches to ongoing monitoring lessens the need for separate evaluations.

Additional Ways This Guidance Will Help Smaller Businesses

The Securities and Exchange Commission (SEC) has noted that internal controls should reflect the nature and size of the company to which they relate. COSO believes the guidance provided herein will assist smaller companies in achieving control effectiveness and managing the associated costs. Companies can accomplish this by:

- *Viewing Internal Control Through a Risk Lens* – Internal control should be viewed within a risk framework.[1] Controls are designed to mitigate material risks. Guidance presented in this document provides illustrations of how a smaller company may link financial reporting objectives and risks to satisfy its control and documentation requirements.
- *Viewing Internal Control as a Whole and Not as Separate Components* – Examples are provided throughout this document that relate to specific principles contained in the *Framework*. An evaluation of internal control should be made on an integrative basis as to whether the components, taken as a whole, create effective internal control over financial reporting. A summary table is included at the beginning of each chapter with

[1] SEC Commission Statement on Implementation of Internal Control Reporting Requirements, May 2005.

key elements for management and auditors to consider in the overall evaluation of each internal control component.

- *Leveraging Examples of Effective Formal and Informal Controls* – Smaller companies already have many elements of internal control in place. Many companies gain assurance that their systems are properly recording transactions by using controls such as prenumbered documents or account reconciliations that contain a certain level of formalization and built-in documentation. These types of controls can be leveraged without significant increases in cost.
- *Developing a Systemic Internal Control Review and Documentation Approach* – The examples included in this report illustrate techniques management may use when developing an overall internal control system. We provide illustrative templates in the appendices to help companies with assessing and evaluating internal control over financial reporting.

Use of This Guidance

Actions taken as a result of this guidance will depend on the position and role of the parties involved. The typical intended audience will include board members, senior management, other personnel, and external auditors.

- *Board Members* – Members of the board of directors can use this guidance as a catalyst for discussion with senior management concerning the state of the company's internal control system and to provide oversight.
- *Senior Management* – This guidance provides the chief executive, chief financial officer and other senior management with suggested approaches that they may considered when designing and evaluating the effectiveness of the company's internal control system. It also provides considerations that can be used in determining the desired formality of controls and requisite documentation.
- *Other Personnel* – Managers and other personnel should consider how their control responsibilities are being conducted in light of this guidance and discuss with more senior personnel ideas for strengthening control. Where a separate internal auditor function exists, it can consider this guidance in relation to evaluations it has undertaken or plan to undertake.
- *External Auditors* – External audit firms can review this guidance to gain a better understanding of how the COSO framework may be applied by smaller public companies. Where practical, it may be used by engagement teams to develop guidelines for acceptable approaches on smaller clients.

We believe this guidance offers a number of benefits. Smaller companies can develop a greater appreciation of how to apply the *Framework* using approaches that reflect their unique operating environments. Management also may be able to limit the amount of incremental effort needed to develop and evidence effective internal control.

Senior management and internal auditors can concentrate on the principles of effective internal control over financial reporting laid out in the Overview Exhibit 1.1 to determine how to appropriately apply the *Framework* to their businesses. A summary of the principles and attributes is presented in Appendix B to assist companies in visualizing how these concepts come together in the form of a matrix or checklist that senior management and the board can utilize for a high-level review of internal control. More detailed guidance is presented in the remaining chapters, including guidance that is specific to control objectives and examples that have been utilized in practice.

The Committee of Sponsoring Organizations of the Treadway Commission

Internal Control – Integrated Framework

Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting

Guidance

1. OVERVIEW

The primary objective of this document is to provide guidance for smaller public companies and their auditors to assist them in applying and implementing the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework* (the *Framework*) as it relates to the effectiveness of internal control over financial reporting. Internal control over the preparation of published financial statements is defined in the *Framework* as a process, effected by a company's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to the reliability of such statement preparation. Secondarily, this document illustrates ways to design and implement effective internal control in a cost-effective manner.

This document supplements the *Framework* and does not supersede or replace it. This guidance articulates principles derived from the original *Framework*. The guidance contained herein is consistent with the *Framework* definitions, components, and criteria for assessing internal control systems and reflects environmental changes and practice improvements that have taken place since the *Framework* was issued in 1992.

While this guidance is provided primarily for smaller public companies, it also may be useful to larger public businesses, private companies, and other organizations in applying the principles contained in the *Framework*.

Sarbanes-Oxley

Many changes have taken place in financial reporting, corporate governance, and the regulatory environment since the *Framework* was issued. Most significantly, the Sarbanes-Oxley Act of 2002 (the Act) was passed by the United States Congress and signed into law by the President on July 30, 2002. Among other provisions, Section 404 of the Act requires management to annually assess and report on the effectiveness of internal control over financial reporting. The guidance contained herein is focused on that objective. Due to unique challenges faced by smaller companies in implementing Section 404 of the Act, and specifically in applying the *Framework* in connection with that effort, the Chief Accountant of the Securities and Exchange Commission (SEC) asked COSO to develop this guidance.

COSO recognizes that Section 404 of the Act is a major driver of companies' evaluation of internal control over financial reporting. Users of this guidance also should remain aware that when using the *Framework* as a basis for reporting pursuant to Section 404, such reporting is done in relation to that document and not this guidance.

Smaller Company Expectations

This guidance resulted from a project commenced by COSO with the goal of identifying approaches that smaller companies might use for achieving effective internal control over financial reporting. COSO learned over the course of this project that, while there are some differences in control approaches, the fundamental concepts of good control are the same whether the company is large or small. Fundamental controls such as reconciliations, management review, and basic input controls remain the same. Thus, there are differences in approaches used by smaller companies versus their larger counterparts in seeking effective internal control. However, the approaches must address the fundamental control principle and often manifests itself in different forms of management review and oversight.

In many instances, the approaches used by a smaller company mirror those of a larger one, although the scale may vary. For example, both smaller and larger companies are likely to develop board oversight responsibilities related to external financial reporting. However, a smaller company may provide less detailed guidance to the board as the nature of the business is less complex. As another example, both smaller and larger companies may institute a whistleblower program. The larger company's version may have more filtering mechanisms to channel information to appropriate personnel than does the smaller company's version. In some instances, while both smaller and larger companies follow similar approaches, albeit on different scales, larger companies may expend significantly more effort than smaller companies in implementing effective internal control over financial reporting.

In certain instances, smaller companies do have unique advantages over larger ones. These can result from wider spans of control and greater transparency to the senior levels of the company. For instance, smaller companies may find informal staff meetings effective for communicating internal control and financial reporting information, whereas larger companies may need more formal mechanisms such as intranet portals, town hall meetings, or peer group conference calls to communicate similar matters.

Notwithstanding, there are also unique challenges presented to smaller business seeking to implement effective internal control over financial reporting. For instance, smaller companies may have greater challenges obtaining sufficient resources, both in terms of funding and staffing, to implement practices such as increasing director's fees and insurance coverage to attract and retain qualified independent directors, hiring qualified senior financial staff, and sourcing an internal audit function.

COSO recognizes this challenge. This guidance provides insights to assist smaller companies in reducing incremental costs associated with current reporting requirements. It provides examples of approaches a small business can take to deal with the small resource

problems. For instance, one approach a small business may utilize involves significant management review of operations. However, that comes with two significant risks – the potential for management override, and less management emphasis on the strategic plan and operations of the business. Management and the organization will need to make a decision on the amount of resources devoted to good internal control to find the most cost effective approach to achieve its objectives over financial reporting.

This document, however, does not provide relief in the form of a short cut to achieving effective internal control over financial reporting. All components of internal control and the related twenty-six principles should be in place in order to achieve effective internal control over financial reporting; however, the scale of the approaches to implement the principles may be different for a small company.

COSO also emphasizes that the *Framework* is principles-based. This document has identified twenty-three principles fundamental to effective internal control for all companies, regardless of size. In addition, the Task Force has identified three principles to assist organizations, and their personnel, in understanding their roles and responsibilities in implementing effective internal control over financial reporting. These are collectively referred to as the twenty-six principles throughout this guidance and all are derived directly from the 1992 *COSO Framework.*

Moreover, this document does not alter the original *Framework* or set a differing level of expectation as to what principles are required for smaller businesses. While all companies should adhere to these twenty-six principles, there are many different approaches used to apply them. This document illustrates, where appropriate, opportunities for companies to enhance internal control over financial reporting using different approaches that will satisfy the twenty-six principles. While these approaches are targeted for smaller companies, many of the approaches are also relevant to larger companies.

COSO urges companies to reduce costs not by reducing the effectiveness of internal control, but by recognizing that internal control over financial reporting may be accomplished by choosing approaches to applying principles that best fit each company's circumstances in the most cost effective manner. The guidance includes in each chapter a discussion of alternative approaches and provides detailed examples taken from smaller companies. The reader is encouraged to look at the approaches and examples and consider the cost effectiveness of these for their organization.

Formalization of Controls and Documentation

A common challenge for smaller companies is to strike a balance between formal and informal controls. Formal controls are those that are performed in accordance with policies established by a company and assist the company in carrying out is control procedures and training personnel. Formalization of controls provides structure and contributes to an understanding of each individual's role and responsibility and thereby enhances the quality of controls. The formalization of controls has the important benefit of creating a source of evidence of the effectiveness of internal controls. Informal controls, on the other hand, are difficult to apply on a consistent basis.

Each company's management must determine the level and form of documentation required for its operations. A question remains as to "how formal" controls must be and, more explicitly, to what extent controls must be formally documented. In addition, management will also establish the formality with which it evidences controls as they occur.

We have considered the formalization of controls in the context of three models.

- **Management reliance only** – When management relies on internal controls solely for running the business, controls and supporting documentation are often less formal, in part due to greater concentration of decision-making authority, wider spans of control, and more direct channels of communication. Although less formal, controls must still be present to meet the company's financial reporting objectives. For example, a smaller company may only verbally communicate internal control weaknesses noted through ongoing monitoring activities, not codify its authority for making decisions as all top management is directly engaged in all key decisions impacting reliability of financial reporting, and may not document key risks potentially impacting the reliability of financial reporting as the same management tasked with identifying risks also manages those risks. Less formal usually implies that the controls are understood but not always formally documented.
- **Management assertion** – When management is required to assert to a third party on the design and operating effectiveness of internal control, it will need information on the design and operation of internal controls. This implies that a company will need to develop greater documentation (more formalization) of controls. For example, a smaller company may verbally communicate to those responsible any control internal control weaknesses noted through ongoing monitoring activities and report quarterly any noted weaknesses to top management. More of the control approaches and management's consideration of weaknesses will be codified. Documentation might include high-level summary diagrams of key risks potentially impacting the reliability of financial reporting.

- **Third-party attestation** – When management is required to have a third party, such as external auditors, attest to the design and operating effectiveness of internal control and key processes, the need for formal documentation and evidence of operation increases to allow the third party to review after the fact. The formality of the documentation must be such that a third party can understand controls in a process and from that information effectively develop tests to determine that controls are working effectively. The formality of the documentation requires that controls are identified with a description of how they work such that an objective party can understand them. In addition, management will have in place more formal requirements to evidence the operation of those controls. For example, a smaller company may communicate via e-mail to those responsible any control internal control weaknesses noted through ongoing monitoring activities and report monthly any noted weaknesses to top management, codify for each member of top management their individual level of authority regarding decisions impacting reliability of financial reporting, and may document using spreadsheets or other tools key risks potentially impacting the reliability of financial reporting.

In determining how to deal with the issue of formal versus informal controls, the COSO Task Force made the following decisions:

- There is no one right approach to achieving effective internal control over financial reporting; that is, a control should accomplish the objective set forth in a principle and there may be many ways to do that.
- Publicly held companies currently are required to provide evidence that controls are working; therefore, this guidance supports implementation of more formal controls when public reporting on internal controls is required.
- The process of understanding and documenting internal control assists companies in mitigating risks.

Organization of This Guidance

Nature of Principles

The *Framework* is principles based. It is not a checklist and it does not imply that the same set of controls must be implemented similarly in every company. This document provides a set of ***basic principles*** derived from the five components of the *Framework* and describes these in boxed text at the beginning of each chapter. The principles represent fundamental concepts associated with each internal control component.

To have effective internal control, a company should implement a mechanism or methodology to accomplish each principle. For example, one principle underlying the control environment relates to developing, communicating, and reinforcing strong ethical values regarding financial reporting. The manner of implementation can be quite different in smaller companies than in larger ones. A large company might require formal signed

statements by all key officers. A smaller company might post in common areas its statement of ethical values, and management might reinforce the values through actions taken at meetings.

The principles identified are derived from the *Framework* and do not represent new concepts. In evaluating each component of the COSO framework, users should consider, on the whole, whether the approaches implemented to achieve the principles satisfy the overall objective related to financial reporting. Stated another way, for each of the components of the *Framework,* judgment is needed to determine whether the principles and approaches taken together are sufficiently robust to conclude that the organization has a control structure that facilitates effective internal control over financial reporting. While we do provide examples of templates, as described on the next page, judgment is required to assess the overall effect of each component on the achievement of effective internal control over financial reporting. When a certain principle is not being met, it needs to be communicated to top management and the board to determine (a) how to address the deficiency, and (b) determine whether the respective internal control components are being met and accordingly, whether the company has attained effective internal control over financial reporting. A failure to achieve one of the principles indicates a weakness in internal control, but it does not necessarily mean that the weakness rises to the definitions of significant deficiency or material weakness as defined by the PCAOB. The organization must consider whether the failure to achieve the principle results in a conclusion that the COSO component is not working and therefore there is a significant deficiency.

Users also should consider the objectives of each principle and relate those objectives to the Public Company Accounting Oversight Board's (PCAOB) definitions of significant and material deficiencies.

Attributes

Supporting each principle are ***attributes*** of the principle. The attributes are characteristics associated with the principles and are generally expected to be present within a company. However, depending on unique factors in each company, it may be possible to accomplish the principle without addressing each individual attribute. The objective is to demonstrate that the principle has been achieved.

The attributes set out in this guidance highlight the integrated nature of the COSO framework. For example, within the control environment component there are attributes of principles that address the communication and monitoring of integrity and ethical values.

Approaches and Examples

Approaches and examples illustrate how actual smaller companies are applying the principles and attributes. Each company may choose to use one or more of the approaches, or it may achieve a principle by developing other mechanisms better suited for its culture and processes.

Finally, examples provided throughout the guidance are based on documented cases from smaller companies observed directly by the Task Force, or that have been provided in other interaction with practitioners. They are intended for illustrative purposes to demonstrate how a specific company addressed the principles; an individual company should consider them to the extent they may be deemed useful. They are not intended to be construed as "best practices" or suggested solutions for all users of this report, and they would not necessarily be sufficient for all companies in all circumstances. Rather, users of this report should focus on making judgments about how to best achieve the principles that underlie the control components and how the principles interact to mitigate the risk of financial statement misstatements or omissions.

COSO believes many users will recognize significant value in the examples that are given. However, each example represents one way to achieve a principle. The best way to address the attributes associated with each principle may vary in different environments and may change over time or as regulations change. Thus, COSO encourages users to focus primarily on the principles. In doing so, readers may discover alternative approaches to effectively accomplish internal control objectives. In other words, the principles (both in the *Framework* and as restated here) are constant, while the approaches and examples, although useful, may be temporal.

Subsequent chapters of this report focus on each of the components of the *Framework*. The reader must keep in mind the need to integrate each component across the risks associated with the underlying processes. The reader also should keep in mind that while the guidance is oriented toward financial reporting, controls established pursuant to operations and compliance objectives also may be relevant to financial reporting.

Templates

The guidance provides in a series of appendices several templates that a company may use as part of its overall evaluation of the effectiveness of internal control over financial reporting. The control matrix presented is one possible tool, but not the only tool, that may be used in determining whether the organization has effectively implemented all key principles included in this guidance. COSO details how these templates can be used as part of a process laid out in Appendix A.

COSO also urges users to recognize that (a) best practices may change over a period of time, and (b) the suggested control procedures are not exhaustive; rather, a company must choose those that best address the control objectives identified.

Implementation of This Guidance

The COSO Task Force has examined ways to simplify implementation of the control concepts in the *Framework*. In doing so, it has developed twenty-six fundamental principles that a smaller business should address in implementing effective internal control over financial reporting. Achievement of these twenty-six principles would demonstrate that controls are in place throughout a company. The operating effectiveness of the controls would be determined by management's assessment and ultimately the external auditors' opining on management's related assertion.

Exhibit 1.1 presents an overview of the basic principles of control contained in the *Framework.* Each principle is derived directly from the *Framework* and is tailored to the objective of implementing effective control over financial reporting. It is recommended top management first identify and evaluate how the twenty-six principles as outlined in the exhibit are in place within the company. Each principle believed to be in place within the company should be evaluated. This will produce a macro perspective of which principles are already in place and which should be adopted as described in this guidance.

Once the assessment of principles has been made, management should determine whether the principles are being achieved, by identifying controls in place that demonstrate accomplishment of the principles. For principles not present, management should determine how best to remediate those deficiencies, develop an implementation plan and maintain communication with external parties.

Exhibit 1.1

Principles Implementation

Framework	Principles	See Page
Control Environment	1. **Integrity and Ethical Values** – *Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for financial reporting.*	26
	2. **Importance of Board of Directors** – *The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.*	29
	3. **Management's Philosophy and Operating Style** – *Management's philosophy and operating style support achieving effective internal control over financial reporting.*	35

Framework	Principles	See Page
Control Environment (Continued)	4. **Organizational Structure** – *The company's organizational structure supports effective internal control over financial reporting.*	37
	5. **Commitment to Financial Reporting Competencies** – *The company retains individuals competent in financial reporting and related oversight roles.*	39
	6. **Authority and Responsibility** – *Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.*	42
	7. **Human Resources** – *Human resource polices and practices are designed and implemented to facilitate effective internal control over financial reporting.*	45
Risk Assessment	8. **Importance of Financial Reporting Objectives** – *A precondition to risk assessment is the establishment of objectives for reliable financial reporting.*	51
	9. **Identification and Analysis of Financial Reporting Risks** – *The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.*	54
	10. **Assessment of Fraud Risk** – *The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.*	58
Control Activities	11. **Elements of a Control Activity** – *Policies and procedures are established and communicated throughout the company, at all levels and across all functions, that enable management directives to be carried out.*	69
	12. **Control Activities Linked to Risk Assessment** – *Actions are taken to address risks to the achievement of financial reporting objectives.*	72
	13. **Selection and Development of Control Activities** – *Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives*.	77
	14. **Information Technology** – *Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.*	81
Information and Communication	15. **Information Needs** – *Information is identified, captured and used at all levels of a company to support the achievement of financial reporting objectives.*	93
	16. **Information Control** – *Information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives.*	95

Framework	Principles	See Page
Information and Communication (Continued)	17. **Management Communication** – *All personnel, particularly those in roles affecting financial reporting, receive a clear message from top management that both internal control over financial reporting and individual control responsibilities must be taken seriously.*	98
	18. **Upstream Communication** – *Company personnel have an effective and nonretributive method to communicate significant information upstream in a company.*	101
	19. **Board Communication** – *Communication exists between management and the board of directors so that both have relevant information to fulfill their roles with respect to governance and financial reporting objectives.*	103
	20. **Communication with Outside Parties** – *Matters affecting the achievement of financial reporting objectives are communicated with outside parties.*	105
Monitoring	21. **Ongoing Monitoring** – *Ongoing monitoring processes enable management to determine whether internal control over financial reporting is present and functioning.*	109
	22. **Separate Evaluations** – *Separate evaluations of all five internal control components enable management to determine the effectiveness of internal control over financial reporting.*	112
	23. **Reporting Deficiencies** – *Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.*	114

In addition to the above twenty-three principles, COSO has identified three principles relating to the roles that various parties play with regard to internal control over financial reporting, and how these roles translate into specific responsibilities. The roles and responsibilities are directly derived from the 1992 guidance.

Roles and Responsibilities	24. **Management Roles** - *Management exercises responsibility and ownership for internal control over financial reporting.*	117
	25. **Board and Audit Committees -** *The board of directors perform their oversight responsibilities relating to the achievement of effective internal control over financial reporting.*	119
	26. **Other Personnel -** *All company staff accept responsibility for actions that directly or indirectly impacts financial reporting.*	121

2. SMALLER COMPANY PERSPECTIVES

Smaller Public Companies and Reporting Responsibilities

A company makes an explicit decision to become public. That decision provides access to the capital markets. However, such access comes with responsibilities for timely and accurate financial reporting to various stakeholders, including:

- Outside capital providers (shareholders, creditors)
- Parties who have direct contractual relationships with the company
- Designated regulatory agencies
- Lending institutions.

COSO recognizes public companies registered with the SEC may or may not be listed on a stock exchange. Regardless, public companies are required to implement a structure of corporate governance and internal control that meets applicable laws and regulations.

Smaller businesses face the same issues as larger companies in determining the set of controls necessary to accomplish their financial reporting objectives. Internal control structures are developed to facilitate growth and contribute to a company's stability over time. Sound controls are designed to support ongoing company operations. Internal control must be cost effective; yet it must address and mitigate significant risks to financial reporting that are inherent within smaller businesses. The guidance contained herein reinforces these concepts: (a) controls contribute to the achievement of company objectives, and (b) controls need to be built in, not merely added on as an extra layer.

Characteristics of Smaller Companies Affecting Internal Control

One of the challenges of providing guidance to smaller public companies is defining what is meant by the term "small(er) business." For example, many think of the local hardware store or a family-owned bakery on the corner as the typical small business. Others may think of a small business as a start-up company, manufacturing a special product that generates $25 million in sales, with hopes that future sales will catapult it to the Fortune 500. Still others see a small company as one that issued its initial public offering 20 years earlier in hopes of future growth, but with a single-product-line manufacturing operation generating annual revenues of $100 million. In some sense, all of these companies may be considered small.

Characteristics versus Bright Lines

While there is a tendency to want "bright lines" to describe a small business, COSO has avoided the temptation to use specific dollar terms in doing so. Additionally, COSO purposefully did not define small businesses using control-related characteristics (e.g., ability to implement adequate segregation of duties, no independent board of directors,

etc.). Effective internal control can be accomplished by all companies, although it may be achieved through different means depending on size.

COSO has chosen to describe smaller businesses in terms of their major characteristics, which include one or more of the following:

- Simple product line and processing
- Founders or a small group of owners who dominate management of the business
- Wider management spans of control
- Economic strategies that often encompass acquiring services on a variable-cost basis as opposed to making fixed-cost investments
- Defined geographic concentration in either production or sales
- Operating size, as measured by revenues, personnel, or assets, that makes it difficult to benefit from the economies of scale larger entities enjoy.

None of these characteristics by themselves are definitive. However, as companies become larger and revenues and assets grow, management will begin taking advantage of more economies of scale and will have narrower spans of control.

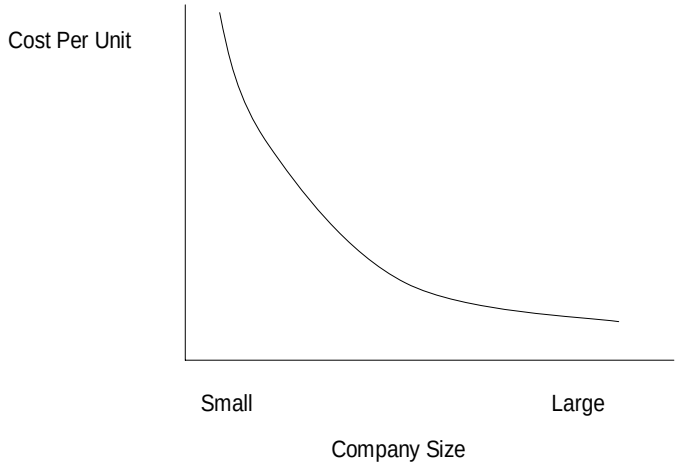
Economies of Scale

In many cases, smaller businesses are lower on the economies-of-scale curve. The curve, as shown in Exhibit 2.1, recognizes that smaller companies often incur higher per-unit costs than do their larger counterparts for activities dependent on some fixed scale of operations. For example, establishing an internal audit function within a hundred-million-dollar company likely would require a larger percentage of the company's assets or revenue than would establishing an internal audit function within a billion-dollar company. Similarly, prior research[2] has shown that smaller companies' accounting costs are a higher percentage of their assets or revenue as compared with larger companies.

[2] See, for example, Larry Rittenberg and R.D. Nair, "Alternative Accounting Principles for Smaller Businesses: Proposals and Analysis," *Journal of Commercial Bank Lending*, April 1983, pp. 2-21.

Exhibit 2.1

Economies of Scale



Smaller businesses, despite their location on the economies-of-scale curve, are competitive and seek out avenues of competitive advantage. Many smaller companies attain cost savings through innovation, lower overhead (fewer people, substituting variable costs for fixed costs), variable compensation plans,[3] and a narrower focus in terms of product, location, and complexity.

Economies of scale may affect how an organization implements control. For example, assume that a board decides it needs an independent, competent internal audit function reporting to the independent audit committee chair. Viewing internal audit as a fixed cost, management and the board might decide it's too costly to build an in-house internal audit function. One alternative is to have members of the audit committee directly conduct independent evaluations of internal control. Another alternative is to outsource the internal audit activity to an established provider of internal audit services, thereby making the cost a variable cost. As another example, project participants[4] indicated that the whistleblowing function can be outsourced cost effectively to companies providing such services. Smaller companies compete by identifying innovative and cost-effective mechanisms within the marketplace. They can utilize the same concepts and innovative

[3] The use of variable compensation plans can increase the risk of fraudulent financial reporting and needs to be considered in the overall context of the company.
[4] See Appendix E – Methodology for a summary of participant involvement.

thinking to accomplish internal control objectives; they cannot, however, reject the need for effective controls simply on the grounds that the company is too small.

Challenges in Implementing Internal Control in Smaller Businesses

Smaller businesses face certain challenges in implementing effective internal control systems, particularly if the business views controls as something to be added on rather than integrated with core processes. These challenges often include:

- Obtaining sufficient resources to achieve adequate *segregation of duties*.
- Management's ability to dominate activities. This increases opportunities for improper *management override* of processes in order to appear that financial reporting objectives have been met.
- Attracting independent, outside parties with financial and operational expertise to serve on the *board of directors* and on the *audit committee.*
- Obtaining *qualified accounting personnel* to prepare and report financial information.
- Controlling *information technology*. Controls over information systems, particularly application and general computer controls, present challenges to smaller businesses.

Segregation of Duties

Segregation of duties means that no single individual has control over two or more phases of a transaction or operation. Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is intended to reduce the opportunities for any one person to be in a position to both perpetrate and conceal errors or fraud in the normal course of his or her duties. Establishing appropriate segregation of duties often presents challenges in small companies.

Segregation of duties is not an end in itself, but rather a means of mitigating a significant risk inherent in processing. In many smaller businesses, one person may have complete control of all aspects of a process, which may increase risks. Segregation of duties is needed so that one individual, or function, acts as a check and balance against the activities of another. For example, if one person processes sales, that person should not have access to processing cash receipts for the payment of receivables, should not be responsible for reconciling the bank account, and should not have authority to write off accounts receivable.

Many smaller companies also develop and deploy compensating controls where resource constraints compromise the ability to segregate duties. Compensating controls are used to counterbalance the potential effect of an internal control weakness and therefore reduce risk of financial misstatement to a relatively low level. Independent reconciliations can provide control to mitigate risks and may be especially important in situations when there is inadequate segregation of duties. In the example above, there is a risk that a salesperson

can provide goods at no or little charge to customers, and then collect money or receive a kickback. As a compensating control, an independent reconciliation of actual inventory on hand with the amount shown by the salesperson would identify a discrepancy. Of course, the reconciliation is only as good as the follow-up investigation to identify the underlying cause of any difference in the account balance. In addition, management reviews the price per unit sold to determine if it is consistent with other recent sales and the suggested list price, and to identify product sold at a discount where the salesperson potentially received some form of kickback.

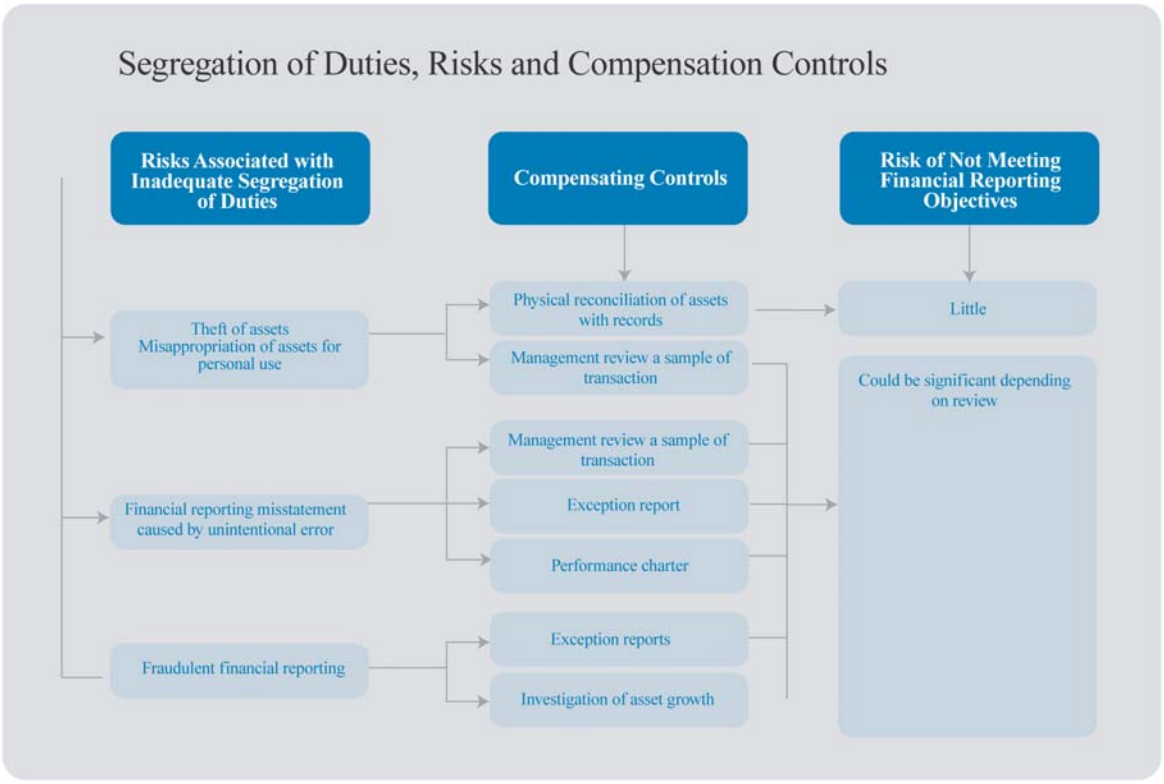
Relying solely on compensating controls is generally less desirable than establishing separation of duties because compensating controls ordinarily occur after transactions are complete. It often takes more resources to investigate and correct errors, and recover losses, than it does to prevent them. However, smaller companies typically have few staff resources, limiting their ability to establish adequate separation of duties. This leaves little choice but to rely more on compensating controls. In these instances, it is important for management to implement controls that compensate for increased risk.

Following are some types of compensating controls a company could implement to address limited segregation of duties.

- *Review reports of detail transactions* – Management may consider reviewing, on a regular and timely basis, reports of detailed transactions initiated by staff who perform all the key activities of the transactions, with limited segregation of duties, to identify, investigate, and correct improper transactions. Using the sales example presented in this section, an adequate review would consider the transaction date, customer, description, dollar amount, and offseting account, if any.
- *Review sample transactions* – A manager could periodically review supporting documents for a sample selected of transactions. The sample could be generated by using detailed reports or data query programs that extract transactions from core systems supporting financial reporting. An adequate review would address the same data above.
- *Take periodic asset counts and comparison with accounting records* – Where there is limited segregation of duties over transactions involving assets such as inventory, equipment or other tangible assets, it may be effective to conduct periodic counts and compare them with inventory records to ensure asserts are on-hand.
- *Review budget analysis and cost trends* – A less effective compensating control is the preparation and/or review of budget and trend analyses of expenditures. While this does not provide a detailed review, it can be a way to identify problem areas where further detailed is needed.

Exhibit 2.2 provides an overview of the risks associated with lack of segregation of duties and examples of compensating controls that might address those risks. The concern for each organization is whether or not the compensating controls reduce the residual risk to an acceptable level. Each organization must consider whether or not the compensating controls (a) address the risks adequately, and (b) are applied conscientiously enough to reduce the residual risk to an acceptable level.

Exhibit 2.2



It often is thought that the manager of a smaller business is in a position to compensate for inadequate segregation of duties due to his/her direct and explicit knowledge of the business. This is appealing because the manager can fulfill such a role without hiring additional personnel. COSO recommends that smaller businesses first explore other alternatives to mitigating risks through segregation of duties before turning to management oversight as a solution.

We make this recommendation because:

- Top management, while having overall responsibility to meet the financial reporting objectives, should concentrate on strategic and operational objectives of the company, and having managers perform some parts of the process results in dilution of

management. Spending time performing operational aspects of financial reporting results in dilution of management's attention to other aspects of the company, such as growing the business.

- There would no longer be an independent check on management's activities, other than the board or audit committee, as discussed earlier.

Management Override

Smaller businesses often are dominated by a founder or controlling owner who contributes to the success of the company while increasing risk of override. The most effective approach to mitigate the risk of management override of internal control starts with the company's commitment to competence and ethical behavior. A commitment to have independent members of the board and to allow them sufficient resources and time to provide effective oversight further enhances outside control. That control is strengthened when:

- An effective whistleblower program exists that provides direct access to the audit committee chair.
- The company has an informed and inquiring audit committee and a board that understands company operations and can identify and diagnose unusual activity potentially impacting financial reporting. Where economically feasible, an effective internal audit activity, or similar function, with sufficient independence reports to the audit committee.
- An audit committee is positioned to take corrective or investigative action arising from an effective independent audit. An independent audit is an effective source of information; however, it is not a company-level control. The company-level control comes from the independent board and its ability to take effective action.

Board of Directors

In some smaller businesses, especially those that have recently become public companies, the top executives may be unaccustomed to sharing governance with outsiders who do not have a substantial stake in the company's operations. Also, smaller businesses may sometimes face challenges in attracting high-quality independent directors. Some smaller businesses may lack high-quality independent directors because of either legal liability issues, or difficulty in attracting and compensating outside directors.

COSO recommends that the board of directors of a public company have a critical mass of independent members who can mitigate the risk of management override of internal control. In addition, the board needs financial expertise in order to objectively review management's judgments and effectively utilize the recommendations of internal and external auditors in evaluating the overall quality of the company's controls.

We have noted large numbers of qualified individuals who are ready and willing to serve on audit committees. Many of these individuals have either extensive experience (retired public accounting firm partners, accounting managers, and CFOs) or a high degree of audit and accounting expertise (professors and chief audit executives of other companies).

COSO believes that even with the added cost of directors' and officers' liability insurance, the advantages of having effective outside board members generally exceed the additional costs and can add significantly to the long-term value of the company. This is not, however, to say that the cost of independent directors is trivial. Good directors can be found if organizations are willing to expand the population from which they generally seek directors. Most directors are committed to providing a significant amount of time to accomplish their responsibilities but reasonably expect adequate compensation for both their expertise and the additional risks they face by serving on a board.

Audit Committees

One change since 1992 has been the emergence of an effective audit committee as a central part of corporate governance. COSO recommends that boards of smaller businesses include an audit committee, composed of independent board members. The audit committee should have authority to engage and provide oversight of the external auditors, and utilize the internal audit function as necessary. Further, we recommend that the chair of the audit committee have a good relationship not only with the CEO and CFO, but also with key accounting personnel (e.g. the controller) so that all important accounting and control issues are brought to the chair's attention.

Qualified Accounting Personnel

Some smaller companies are challenged in obtaining qualified personnel not at the clerical or administrative level, but at higher levels, where a greater understanding of accounting principles is required. Many smaller businesses historically have held conversations with their external auditors regarding appropriate accounting practices and in some cases have asked for guidance on how to appropriately adopt them. These businesses can and should continue to have discussions with their external auditors, as well as with others who can help them deal with complex accounting issues. However, smaller companies need enough expertise for management to make its own decisions based on external advice.

Information Technology

The level of effort required to establish effective internal control over information technology is largely, although not completely, a reflection of the extent of standard, packaged software versus custom, in-house developed software. Fewer controls over change management are needed when companies use standard, highly-regarded accounting packages that do not allow users to modify programs than when companies rely on in-house software under the direct control of only a few individuals.

The extent of user-defined access within a computer application, whether from a third party or developed internally, has important control implications. A system that provides for standard access profiles requires fewer access-focused controls than do systems that allow users considerable latitude in configuring access profiles.

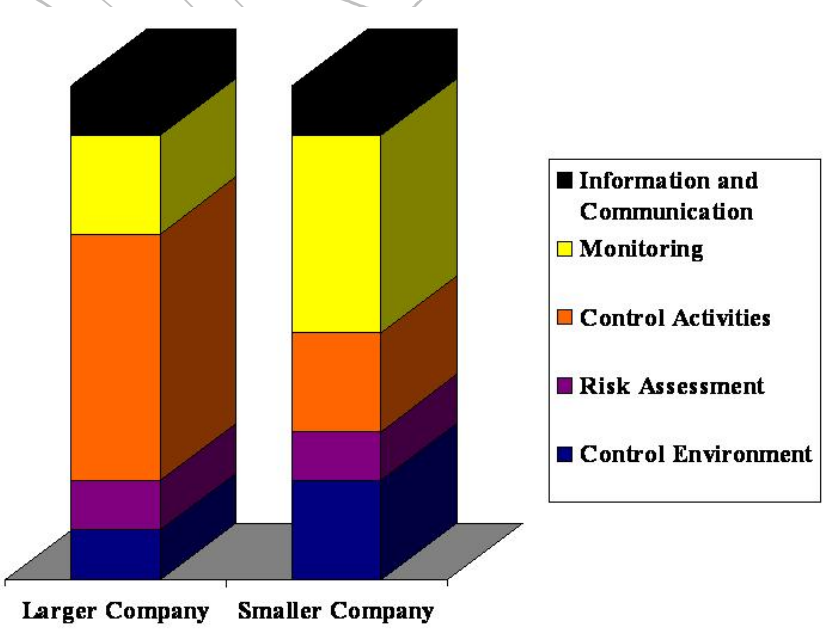
Further, packaged programs often include built-in controls and documentation, allowing a smaller business to rely on those controls and facilitating the review of documentation.

How Smaller Companies Can Use the *Framework* Components to Achieve Effective Internal Control

Not every company, large or small, will apply internal control in the same way. Looking at the ways smaller companies versus larger companies generally apply the five components of the *Framework*, we do see a common distinction.

Companies must implement a control structure to reduce risk to an acceptable level. Sometimes, smaller companies do not perceive that they have sufficient resources to fully implement segregation of duties or other controls that are more preventive in nature. Thus, smaller businesses may rely more on "after the fact" monitoring and personal involvement by top management in setting a control environment that brings in sufficient competence and trust to assist in reducing risk. This is illustrated broadly in Exhibit 2.3. All companies, regardless of size, needs to have all five components present and functioning, but the relative reliance on each component may be different in smaller companies than it is in larger companies.

Exhibit 2.3



Smaller companies often increase reliance on the control environment, as there is more direct oversight and reinforcement of the "tone at the top" by management. Management may rely more on its control environment to deter override of internal control and to partially compensate for deficiencies in other areas, including inadequate segregation of duties. The important question is whether the combination of controls reduces residual risk to a reasonably low level. Further, management of smaller businesses, in which top management have a direct and explicit knowledge of activities, often places greater emphasis on monitoring functions. For smaller companies, executives have a direct and explicit knowledge of activities, thereby allowing them to place more reliance on monitoring than on control activities.

While there may be less direct reliance on control activities in smaller companies, there are certain foundational control activities that need be in place in every company. Both smaller and larger companies will have similar control activities including reconciliations of key accounts, approvals of large transactions, and various input controls.

Account Balances Are Not Just Transactions Based

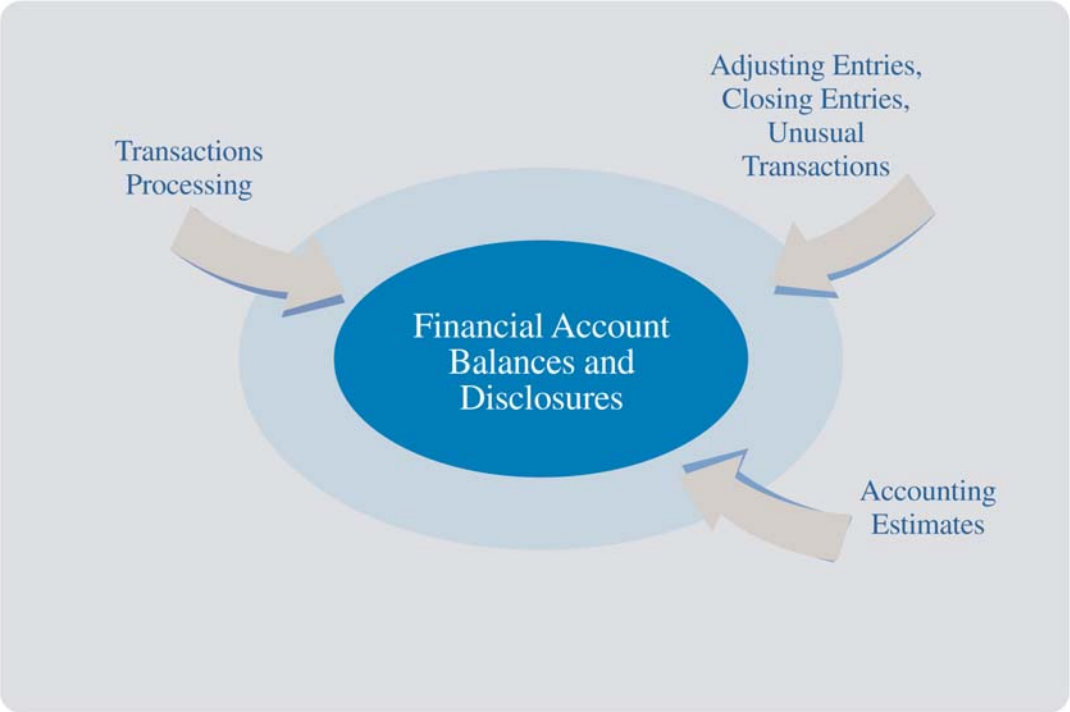
Financial account balances are affected by three broad sets of processes, namely:

- Transaction processing systems
- Accounting estimates and underlying systems, processes, and information supporting these estimates
- Adjusting entries, closing entries, and unusual transactions.

A simplified view of the processing leading to transparent financial reports is shown in Exhibit 2.4.

Exhibit 2.4

Processes Leading to Financial Reports



There are significant risks associated with each of these processes. For example, the adjusting and closing entry process is susceptible to management override. In fact, many of the business and control failures of the past decade have been attributed to improper accounting estimates and adjusting entries. Accounting estimates are often dependent on a thorough analysis of the economic environment, and in some cases the actions of competitors, and are susceptible to manipulation. Transaction processing systems are subject to numerous risks, ranging from failure to accurately capture all authorized transactions, contamination through unauthorized transactions, and incorrect processing. Appendices to this guidance also include sample matrices that may be used to assist in the evaluation of each of the processes leading to financial reporting, as noted above.

One way to approach the review of these financial reporting processes is to:

- Identify material account balances and the flow of information that affects each account balance and related disclosure
- Analyze the account balances that are material
- Identify financial reporting assertions and risks associated with each account balance

- Evaluate the adequacy of controls over the process and their ability to reduce the risks to an acceptable level.
- Conclude on overall effectiveness of internal control over financial reporting

This approach, along with potential tools is further detailed in Appendix A.

Controls Are Integrated and Principles Based

The *Framework's* five components comprise internal control principles. There is synergy and linkage among these components and related principles, forming an integrated system that reacts dynamically to changing conditions. While the principles are the same for each company, how the principles are applied varies.

COSO encourages readers to recognize that internal control is broader than the objectives related to financial reporting. Internal control includes objectives related to the efficiency and effectiveness of operations and compliance with laws and regulations. While it may be possible to separately identify and segregate controls that are related to financial reporting processes, it is important to understand that the *Framework* is a fully integrated framework and that information needed for financial reporting may come from operations or the company's processes to ensure compliance with important laws or regulatory requirements.

Determining Effectiveness in a Smaller Business

Many businesses shifting from an informal to a formal approach to evidencing internal control will follow a process whereby they identify and assess current internal controls, identify and remediate deficiencies in current processes, and then put in place mechanisms to maintain internal control over the longer term, as described below.

- *Identify and evaluate current internal controls* – This includes an assessment of how internal control components, principles, and attributes currently are being applied within processes and across the entity. The company also identifies formal and informal processes, policies, procedures, and practices currently in place, as well as existing capabilities in the company for applying the *Framework* principles. This may be done, perhaps through discussion with key process owners, using Exhibit 1.1. This allows management to draw preliminary conclusions of whether its current controls reduce risks to the company's financial reporting objectives to a relatively low level. The evaluation also assists in avoiding duplication and is an important step in achieving efficiency and cost savings.
- *Identify deficiencies* – The evaluation of current internal controls provides insights about processes that need strengthening or development. Deficiency remediation may include defining roles and responsibilities, as well as approaches that might be used to improve internal controls. These often include modifications to the organizational model, methodologies, tools, techniques, information flows, and technologies.

- *Implementation plan* – Actions are developed, or updated, as needed to implement and sustain the internal control system, including evaluation and testing plans, training sessions, reward reinforcement mechanisms, and monitoring of the remainder of the implementation process.
- *External party coordination* – During this phase, management facilitates open dialogue with external parties, including external auditors and providers of outsourced services. It is essential providers of outsourced services understand how they fit into the internal control structure and what they will be expected to contribute to the implementation. A periodic meeting with the external auditors is encouraged to facilitate an effective and efficient execution of the internal control attestation process required for public companies under the Act.

To assist with the above process, management may use the templates provided in the appendices. This control matrix is one possible tool, but not the only tool, that may be used in determining whether the organization has effectively implemented all key principles included in this guidance. The appendix provides a template for entity-level controls, one transaction cycle, adjusting entries and accounting estimates.

3. CONTROL ENVIRONMENT

The control environment component is the foundation upon which all other components of internal control are based. A strong control environment, particularly in a smaller company setting, can partially compensate for internal control deficiencies in other areas and often is viewed synonymously with the "tone at the top." Research continues to provide evidence that companies perform better and last longer when a commitment to strong internal controls is made by members of top management and clearly conveyed through their actions.

Employees in smaller businesses, unlike in their larger counterparts, often interact with top management and typically are directly influenced by management actions. Therefore, management more effectively reinforces the fundamental values of the company by how its members act, especially with respect to policy. Employees follow their lead; and when there is inconsistency between words and actions, employees most often are guided by their leaders' actions.

The most efficient and cost-effective way to implement and assess internal control over financial reporting is to build control consciousness into the culture of a company. When controls are built into the company, they become part of its fabric, and problems are identified and dealt with in a timely fashion. Unintentional error and unethical acts are identified and reported through formal and informal channels. The controls and corrective actions taken can be documented by simply recording the problems and their dispensation.

Control Environment Principles

The control environment represents a company's first line of defense to mitigate the risks of financial reporting misstatements. COSO has identified seven major principles related to the achievement of control objectives at the control environment level. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section I of Appendix B.

1. ***Integrity and Ethical Values –*** Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for financial reporting.
2. ***Importance of the Board of Directors –*** The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.
3. ***Management's Philosophy and Operating Style –*** Management's philosophy and operating style support achieving effective internal control over financial reporting.
4. ***Organizational Structure –*** The company's organizational structure supports effective internal control over financial reporting.

5. ***Commitment to Financial Reporting Competencies –*** The company retains individuals competent in financial reporting and related oversight roles.

6. ***Authority and Responsibility –*** Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.

7. ***Human Resources –*** Human resource polices and practices are designed and implemented to facilitate effective internal control over financial reporting.

The remainder of the chapter articulates each of these principles along with the fundamental attributes that are normally associated with the successful implementation of the principle as it affects the achievement of effective internal control over financial reporting. Each chapter then describes approaches that smaller companies may consider in achieving the principle. The approaches are not prescriptive, rather than simply represent a menu of alternatives an organization may consider. Next, each chapter provides specific examples that smaller businesses have taken to implement the principle.

Integrity and Ethical Values

Basic Principle

Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for financial reporting.

Attributes of the Principle

- *Developed* – Top management develops a clearly articulated statement of values or ethical concepts that are understood by key executives and the board.
- *Communicated* – Top management communicates its commitment to ethical values and reliable financial reporting through words and actions.
- *Reinforced* – The importance of integrity and ethical values is communicated and reinforced to all employees in a manner suitable for the organization.
- *Monitored* – Processes are in place to monitor the company's compliance with principles of sound integrity and ethical values.
- *Deviations Addressed* – Deviations from sound integrity and ethical values are identified in a timely manner and are addressed and remedied by appropriate levels within the company.

Approaches Smaller Companies Can Take to Achieve the Principle

- The CEO and key members of management demonstrate the importance of sound integrity and ethical values to employees through their:
  - Day-to-day actions and decisions that demonstrate sound integrity and ethical values
  - Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings
  - Design of performance appraisals and other incentives that diminish temptations inconsistent with financial reporting objectives
  - Intolerance of ethical violations at all levels.
- The company implements mechanisms to inform new employees and remind current employees of the company's objectives related to integrity and ethics, and corporate mission and values. Such mechanisms include:
  - Providing information to new hires emphasizing senior management's views about the importance of sound integrity and ethics
  - Periodically providing employees updated information relevant to maintaining sound integrity and ethical values
  - Making ethics guidelines available in hardcopy or electronic form
  - Including periodic training or other formal discussions that review current and new policies related to sound integrity and ethics

  - Periodically receiving confirmations from employees documenting their level of understanding of key principles.
- Communications channels exist to inform employees about how to report behavior that is inconsistent with the company's ethics guidelines. Such communications channels include:
  - Whistleblower or similar mechanisms to report potential violations
  - Access to independent parties (e.g., through secured Internet/intranet sites or email) who are responsible for dealing with submitted complaints
  - Direct lines of communication to external legal counsel or other board-designated recipients.
- Employees' actions that positively reflect sound integrity and ethical values are rewarded and recognized (for example, through performance reviews or public recognition programs).
- Management demonstrates the importance of sound integrity and ethical values by following an identified process and taking appropriate, timely corrective action when violations are identified. For example, management takes actions such as:
  - Investigating occurrences of possible violations to gain a thorough understanding of the issues and circumstances
  - Documenting the occurrences
  - Remedying the situation appropriately and in accordance with prescribed company guidelines on a consistent and timely basis
  - Following up to support continued compliance.

Examples of Effective Ways to Achieve the Principle

Using Company Newsletter to Reinforce Integrity and Ethics

A company emphasizes the importance of exercising sound integrity and ethical values in its monthly newsletter distributed to all employees. Each newsletter contains a section related to ethical decision making, which emphasizes key aspects of the company's mission statement and ethical values and includes examples of ethical dilemmas, with suggested resolutions. The newsletter reminds all employees that, as part of their annual performance review, they must certify that they have read the company's mission statement and policies related to ethics and are in compliance with those policies.

Promoting Awareness of Ethical Behavior

A company promotes awareness of its expectations for ethical behavior as a part of regularly scheduled employee meetings. At these meetings, key components of the code of conduct are discussed. Evidence supporting these discussions includes meeting notifications, agendas, or session presentations.

Aligning Incentives with Ethics and Values

A company structured its bonus plan to have 30% of the potential incentive award be directly related to the demonstration of the company's core values. Specific comments on how management does and does not reflect values are captured through upward feedback mechanisms. During the employee performance review and appraisal process, management provides feedback about the extent to which each employee has performed in accordance with the company's core values for sound integrity and ethics.

Promoting and Reinforcing a Commitment to Ethics

A company promotes its commitment to ethical behavior through a code of conduct, made available to all employees and third parties on its website (or via compact disks). As evidence that information about expectations for ethical behavior is communicated effectively throughout the organization, each employee is required to review the corporate code of conduct and sign a confirmation that he/she read the code and is in compliance with its provisions. The signed confirmation is retained in the employee's file. The code of conduct contains information on how to report a policy violation through an independent third party for review and follow-up.

Promoting Employee Participation in Identifying Misconduct

A company promotes the reporting of ethical misconduct by providing an anonymous help line for employees to discuss potential fraud occurrences and other ethical concerns, without fear of reprisal. The company engaged a third-party service provider to proctor the help line. The annual cost to the company is minimal. Potential illegal acts or financial reporting improprieties identified by this help line are reported directly to the audit committee and general counsel. The audit committee's review and discussion of call reports and follow-up actions provide evidence that the help line is functioning.

Taking Actions When Deviations Occur

A company learned that the accounts receivable clerk, an employee for 15 years, was misapplying customer credits to cover up an embezzlement of cash. The employee was immediately confronted, access privileges were suspended temporarily, and a full investigation was launched. Once the impropriety was confirmed, the company terminated the clerk, permanently revoked all access and privileges, and filed formal charges with the appropriate authorities. The company documented the situation, including its resolution and that resolution was clearly communicated across the company.

Importance of Board of Directors

Basic Principle

The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.

Since 1992, corporate governance has evolved such that audit committees perform most of the activities noted below. COSO recommends companies form an active audit committee of independent members with financial expertise. When a company chooses not to have an audit committee, it should have independent board members with financial expertise that perform the activities below.

Attributes of the Principle

- *Evaluates and Monitors Risk* – The board of directors actively evaluates and monitors:
  - The risk of management override of internal control
  - Risks affecting the reliability of financial reporting.
- *Oversees Quality and Reliability* – The board of directors, through its independent audit committee, provides oversight responsibility related to he effectiveness of internal control over financial reporting and the preparation of financial statements for external purposes.
- *Oversees Audit Activities* – The audit committee oversees the work of all audit functions, including, internal audit, and external auditors, and interacts with regulatory auditors, as necessary. The audit committee has the exclusive authority to hire, fire, and determine the compensation of the external audit firm.
- *Independent Critical Mass* – The board of directors has a critical mass of members who are independent of management.
- *Independence of Audit Committee* – The audit committee is constituted solely of independent members of the board.
- *Financial Expertise* – The board of directors and audit committee have one or more members who have financial expertise.
- *Frequency* – The board of directors and its audit committee meet regularly, often in executive sessions and devotes sufficient time and resources to adequately carry out its functions.

Approaches Smaller Companies Can Take to Achieve the Principle

- The company identifies independent board and audit committee members through sources available to smaller businesses:

  - The American Institute of Certified Public Accountants (AICPA) maintains a listing of qualified certified public accountants (CPAs) who have expressed an interest in being board and audit committee members
  - The Financial Executives International (FEI) also maintains a listing of potential directors
  - Retired public accounting firm partners in most U.S. cities (including small cities) who have expressed an interest in becoming audit committee members
  - Internal auditors who have expressed an interest in serving as audit committee members (chief audit executives from larger organizations often can bring very useful operational perspectives to smaller businesses).
  - Accounting academics, a largely untapped resource that also can add value to most organizations
  - Controllers and CFOs of other smaller and mid-sized as well as larger organizations also can serve as effective board and audit committee members
  - Members listed with the National Association of Corporate Directors.
- The board of directors or audit committee regularly discusses the effectiveness of internal control over financial reporting, including consideration of emerging risks, significant deficiencies, and material weaknesses (if any).
- The board of directors or audit committee reviews accounting policies and procedures used by management for determining significant estimates, including key assumptions made by management in establishing those estimates.
- The board of directors and audit committee maintain an appropriate level of skepticism regarding management assertions and judgments affecting financial reporting by asking difficult and probing questions of management.
- The board of directors or audit committee reviews the financial statements before releasing them externally.
- To monitor the risks of management override of internal control, the board of directors or audit committee considers information obtained from whistleblower or similar processes.
- The board of directors conducts due diligence procedures about potential board member candidates to confirm a candidate's independence from the company and ability to be an effective board member. Such procedures include:
  - Performing background checks
  - Obtaining independent references
  - Reviewing all current affiliations/directorships
  - Reviewing information about financial and other relationships the potential board member has with the company and its external auditors
  - Using an independent nominating committee or search firm to oversee due diligence procedures

  - Monitoring performance of due diligence procedures by independent directors.
- The company requires each board member to certify annually his/her compliance with the company's ethics guidelines and to provide information about his/her independence from the company and its external auditors.
- The board of directors and audit committee allocate a portion of every meeting for discussions of issues without management present, including time with external advisors (for example, the external auditors or outside legal counsel).

Examples of Effective Ways to Achieve the Principle

Reviewing and Documenting Key Activities of the Board

A company's board of directors reviews budgets, requires management explanations for significant variances, and participates in approving all major business decisions having material financial reporting implications, such as acquisitions, major capital expenditures, bonus and incentive arrangements, and contractual arrangements with significant vendors/suppliers. The board, through its audit committee, engages the external auditors, reviews audit plans, and assesses effectiveness of the board and review management's assessment of the control environment and financial reporting process. Further, the board of directors is apprised, on a timely basis by management, of the company's approach for adopting new accounting guidance that significantly impacts financial reporting. Evidence that the principle is in place is documented by:

- The board of directors, through the corporate bylaws, and the audit committee, through its charter, outlining their scope and responsibilities, and amending those documents as needed.
- For all board meetings, maintaining minutes (or a summary of the meeting) that record discussion points and resolutions.

Aligning Audit Committee Practices with the Committee's Charter

A company's audit committee has a charter that it uses to establish its meeting agendas. The audit committee chair assigns each audit committee responsibility identified in the charter to at least one audit committee meeting during the year. The audit committee chair also submits draft agendas for upcoming meetings to other members of the audit committee and the external auditors to seek feedback about the need for additional agenda items.

Audit Committee's Independence and Financial Expertise

A company has an audit committee with three independent members. The audit committee chair is independent and also possesses financial expertise (she is a CPA and has previous public accounting experience). The audit committee chair has developed a candid and ongoing dialogue with the external audit engagement partner.

Audit Committee Evaluating Certain Judgments and Estimates

A company's independent audit committee meets regularly with management to discuss judgments and assumptions made by management related to key financial statement accounts and disclosures. The audit committee reviews the reasonableness of management's judgments and assumptions used to develop significant estimates. In addition, the audit committee meets with the external auditors to discuss their assessment of management's estimates and the related impact on the financial reporting process. A portion of each audit committee meeting, including meetings via teleconference, is reserved for executive session.

Audit Committee Interacting with External Auditors

A company's audit committee meets with the external auditors in executive session at least annually, to allow the audit committee and auditors the opportunity to discuss without management present issues such as internal control over financial reporting, significant adjustments to the financial statements, and quality of financial reporting. Further, the audit committee is directly responsible for the hiring, monitoring, and, if needed, termination of the company's external auditors.

Audit Committee Considering Management Override of Controls

The audit committee discusses, in executive session at least annually, its assessment of the risks of management override of internal control, including discussion of why management might override controls and how it would conceal its activities. Audit committee members occasionally make inquiries of members of management not responsible for financial reporting (such as sales managers, procurement managers, human resource managers, and so forth) to seek information about any possible concerns about ethics and any management override of internal controls.

Changing Board Composition of Closely Held Company

A company is registered with the SEC and trades on the OTC exchange. Throughout its history as a public company, it has maintained a board of directors that includes two management directors, three relatives of the company's CEO and founder, and three outside (but not independent) directors (including the company's outside counsel, a representative of the company's banker, and a personal friend of the CEO and founder). To improve its control environment and strengthen the effectiveness of its board, the company reconstituted its board as follows: The relatives and personal friend of the CEO and founder left the board, and two independent directors were added to the board. One of the independent directors possesses financial expertise. The company identified the two

new independent directors by accessing directories of potential board members maintained by the National Association of Corporate Directors, Financial Executives International, and American Institute of Certified Public Accountants.

Audit Committee Setting Meeting Contents

The audit committee establishes a calendar of topics for review and consideration over its fiscal year. This helps the board, through the audit committee, provide oversight of internal control and helps management anticipate and plan for audit committee expectations.

	Frequency			Planned Meeting			
				Quarter			
	A	E	AN	1	2	3	4
Audit Committee Issues							
Report results of annual independent audit to the board	✓			✓			
Appoint the independent auditors	✓			✓			
Approval of independent auditor fees for upcoming year				✓			
Review annual proxy statement audit committee report and charter	✓			✓			
Assess the adequacy of audit committee charter	✓				✓		
Approve audit committee meeting planner for the upcoming year, confirm mutual expectations with management and the auditors	✓				✓		
Perform Audit Committee Self Assessment					✓		
Approve any non-audit services provided by outside auditors			✓				
Approve the Guidelines for Engagements of External Auditors for Other Services (preapproval policy)	✓			✓			
Report of external auditor pre-approval status/limits		✓		✓	✓	✓	✓
Review the procedures for handling reporting violations	✓				✓		
Approve minutes of previous meeting		✓		✓	✓	✓	✓
Report quarterly matters to the board (chair)		✓		✓	✓	✓	✓
Executive session of committee members			✓				
Other matters			✓				
Other Members of Management							
Legal matters (General Counsel)							
Conflict of interest and ethics policies	✓				✓		
Litigation status/regulatory matters			✓				
Information systems matters (IT Manager)			✓				
Risk Management Manager			✓				
Tax matters (Tax Manager)			✓				
Others			✓				

A = Annually; E = Each Meeting or Conference Call; AN = As Necessary

Audit Committee Setting Meeting Contents

The audit committee establishes a calendar of topics for review and consideration over its fiscal year. This helps the board, through the audit committee, provide oversight of internal control and helps management anticipate and plan for audit committee expectations.

	Frequency			Planned Meeting			
				Quarter			
	A	E	AN	1	2	3	4
Financial Management							
Annual Report, 10-K, and Proxy Statement Matters	✓			✓			
Quarterly Report Earnings Review with external auditor & management (1), Form 10-K matters (if applicable) Preapproval of external auditor professional activities		✓		✓	✓	✓	✓
Assessment of internal control environment and systems of internal controls	✓			✓			
Status of significant accounting estimates and judgments (e.g., reserves) and special issues (e.g. major transactions, accounting changes, SEC issues, etc.)			✓				
Other matters (adequacy of staffing, succession planning, etc.)			✓				
Executive session with management			✓				
Independent Auditors							
Results of annual audit (including required communications)	✓			✓			
Results of timely quarterly reviews (including required communications)		✓		✓	✓	✓	✓
Report on material internal control weaknesses and other recommendations and management response, if applicable			✓				
Scope of annual audit	✓			✓			
Required written communication and discussion of independence (SAS 61 & ISBS 1)	✓			✓			
Other matters (adequacy of financial staff, succession planning, etc.)			✓				
Executive sessions with independent auditors			✓				
Internal Auditor / Risk Assessment							
Scope of internal auditing plan for upcoming year	✓						✓
Coordination with independent auditors /outsource auditors			✓				
Defalcations and irregularities – hotline activity		✓		✓	✓	✓	✓
Summary of significant audit findings and status update relative to annual plan		✓		✓	✓	✓	✓
Executive session with internal audit risk assessment			✓				
A = Annually; E = Each Meeting or Conference Call; AN = As Necessary							

Management's Philosophy and Operating Style

Basic Principle

Management's philosophy and operating style support achieving effective internal control over financial reporting.

Attributes of the Principle

- *Set the Tone* – Management's philosophy and operating style emphasize high-quality and transparent financial reporting.
- *Articulate Objectives* – Management establishes and clearly articulates financial reporting objectives, including those related to internal control over financial reporting.
- *Select Principles and Estimates* – Management follows a disciplined, objective process in selecting accounting principles and developing accounting estimates.

Approaches Smaller Companies Can Take to Achieve the Principle

- Management emphasizes the importance of minimizing risks related to financial reporting in its interactions with others involved in the financial reporting process, and through its actions with customers, suppliers or distributors, and employees.
- Management discusses financial reporting objectives, including objectives related to fair, accurate, and reliable financial reporting, with those involved in the financial reporting process.
- The company's operating philosophy requires that all material journal entries be properly authorized and supported by adequate documentation, and that all material accounting estimates be supported by adequate documentation and subject to appropriate review by the company's controller or CFO.
- Management emphasizes to employees the importance of applying appropriate skepticism and business judgment in the performance of assigned job responsibilities.

Examples of Effective Ways to Achieve the Principle

Reinforcing the Tone for Effective Financial Reporting

A high-growth company uses an aggressive operating style to achieve the company's short-term goals. To monitor risks associated with this aggressive approach to managing the business and to minimize opportunities for aggressive and inappropriate financial reporting, senior management and the board of directors actively monitor the actions of operating managers and have instituted other monitoring mechanisms (such as an outsourced internal audit group). In addition, they continually remind employees of lack of tolerance for unethical behavior.

Soliciting Suggestions During Performance Reviews

A company encourages all employees to submit suggestions for improvements in internal control over financial reporting by soliciting such suggestions as part of the annual performance evaluation process. Employees are rewarded for providing effective suggestions that improve internal control over financial reporting.

Emphasizing Philosophy with External Parties

As part of its standard contracting processes with key customers, suppliers, vendors, and consultants, the company emphasizes in all contracts with external parties its commitment to excellence and ethical conduct; and encourages external parties to notify the company's general counsel if suspicions arise about questionable employee actions. Contracts provide information about mechanisms external parties can use to provide the information.

Organizational Structure

Basic Principle

The company's organizational structure supports effective internal control over financial reporting.

Attributes of the Principle

- *Establishes Responsibility* – Management establishes internal reporting responsibilities for each functional area and business unit in the organization.
- *Maintains Structure* – Management maintains an organizational structure that facilitates effective reporting and other communications about internal control over financial reporting among various functions and positions of management.
- *Maintains Processes* – Management's lines of reporting recognize the importance of maintaining processes for objective verification of information reported to the public.

Approaches Smaller Companies Can Take to Achieve the Principle

- Each unit or function within the organizational structure aligns roles to key processes supporting financial reporting objectives.
- Significant processes are documented to explain the flow of transactions, controls to address key risk areas, and related reporting responsibilities.
- Management prepares job descriptions for key positions and updates these during the annual review process.
- Illustrations, such as flowcharts and diagrams, highlight reporting responsibilities across the entire organization.

Examples of Effective Ways to Achieve the Principle

Establishing Job Descriptions and Responsibilities

The CEO requires each business unit manager to maintain documented job descriptions and reporting responsibilities for each position in the business unit. Organization charts are established in each business unit and periodically updated and maintained to illustrate each position and all lines of reporting within the business unit.

Reorganizing to Support Control Structure

Before a company became public, its employees reported to the owner/CEO. Upon the company becoming public, senior management wanted to strengthen its organizational structure. Management created three general departments – sales and customer service, purchasing/inventory, and accounting – to oversee its core business activities. Managers were put in charge of these departments and internal controls were established. Formal job

descriptions were documented and updated to enable a full understanding of each person's role within the organization. Documentation of major cycles also was developed to highlight key controls and each person's responsibility in those processes. In addition to strengthening the delineation of the organizational structure, the CEO wanted to maintain an open culture. The CEO assured all employees that an "open door" policy existed, thereby encouraging the free flow of information across the organization.

Commitment to Financial Reporting Competencies

Basic Principle

The company retains individuals competent in financial reporting and related oversight roles.

Attributes of the Principle

- *Identifies Competencies* – Competencies that support accurate and reliable financial reporting are identified.
- *Retains Individuals* – The company employs or otherwise utilizes individuals who possess the required competencies related to financial reporting.
- *Evaluates Competencies* – Needed competencies are regularly evaluated and maintained.

Approaches Smaller Companies Can Take to Achieve the Principle

- Before hiring for key financial positions, the company establishes and agrees on the knowledge, skills, and abilities (and related credentials) needed to effectively discharge the positions.
- In situations where multiple competencies are provided by one individual, management establishes processes for effective oversight by supervisory personnel to achieve financial reporting objectives.
- The company supplements in-house financial reporting competencies by establishing outsourcing arrangements with specialists or consulting with public accounting firms or other consulting firms on accounting and financial reporting matters, as permitted by regulatory standards.
- Management provides training programs for employees involved in financial reporting processes, either in-house or through outside vendors.
- The board of directors or audit committee evaluates the competencies of individuals serving in key financial reporting roles, such as CEO and CFO.
- Management periodically reviews and evaluates employees relative to their assigned jobs to determine whether the employees' skills are appropriate for their current job responsibilities.

Examples of Effective Ways to Achieve the Principle

Assessing Key Financial Reporting Personnel

At least annually, a company undertakes a process to assess the competencies and skill sets of its key financial reporting personnel. The company leverages the role and knowledge of its external auditors and their interaction with members of the organization. Accordingly, when the audit committee meets privately with the external auditors, the audit committee chair requests specific feedback regarding their assessment of the competencies, skill sets, and performance of the key members of the financial reporting team. Based on this assessment, the audit committee chair discusses key comments with the board of directors and recommends any needed actions. Management utilizes this input in planning staffing. This process, and personnel changes that occur as a result of it, are documented in the minutes of the board of directors' meetings.

Seeking Support for Implementation of Complex Technical Matters

A small high-tech company, which operates in a niche industry, makes extensive use of stock options in compensating its employees. The company has an individual who fills the roles of both CFO and controller. Although this individual is generally competent in applying key elements of GAAP, the individual is not adept at applying some of the recently-issued complex technical pronouncements. Management engaged in dialogue with its external auditors to understand the requirements of the new pronouncements. To avoid the cost of hiring an additional employee, the company considered:

- Providing training for the individual to develop the needed competencies
- Outsourcing the initial implementation of new standards to a third-party expert, with the expectation that in-house personnel would be able to apply the standards in future years.

The company decided that providing training was the more cost-effective alternative.

Utilizing Outside Service Provider

A company prepared a cost–benefit study of performing payroll and 401(k) plan administrative duties in-house, versus having an outside service provider perform these tasks. It was determined there was a significant economic benefit to having an independent party perform these duties. Additionally, use of the third party improved needed segregation of duties and enhanced company access to qualified specialists. The company obtains and considers SAS 70 internal control-related reports issued by the third party's auditor to evaluate whether appropriate controls are in place.

Aligning Competency with Key Financial Reporting Positions

A local start-up company nearly doubled its annual sales volume over a period of a few years. The company's controller, who was hired initially to perform basic accounting and bookkeeping functions, soon found that financial statement estimates and adjustments required due to the company's growth were beyond his expertise and training. Because this individual contributed effectively to many basic financial reporting processes, the company decided to align his skills with a far more suitable position. Another individual with the needed competencies was hired as the new controller, which provided the necessary competencies for the position as prescribed by the board of directors. The company relied on its hiring policies manual, which outlined the process for hiring qualified and competent individuals. Additionally, each employee's personnel file documents the basis for his/her initial hiring and the review and evaluation of the employee's job performance on an annual basis.

Providing Adequate Technical Training

A company sent three managers to external specialized training. These managers subsequently held an on-site training session for the employees in their respective departments. This approach to training allowed the organization to receive relevant, up-to-date technical accounting information in a cost-effective manner. Additionally, other course offerings and descriptive outlines of training opportunities are made available to all employees so they are aware of company-supported training opportunities. Documentation of training attended is included in employee files, which provide evidence of the company's commitment to developing the competence of its personnel.

Authority and Responsibility

Basic Principle

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.

Attributes of the Principle

- *Board Oversees Financial Reporting Responsibility* – The board of directors oversees management's process for defining responsibilities for key financial reporting roles.
- *Defined Responsibilities* – Assignment of responsibility and delegation of authority are clearly defined for all employees involved in the financial reporting process.
- *Limit of Authority* – Assignment of authority and responsibility includes appropriate limitations.

Approaches Smaller Companies Can Take to Achieve the Principle

- For key financial reporting positions, the board of directors reviews and approves descriptions of the positions' responsibilities and authorities, and considers how those positions affect the strength of internal control over financial reporting.
- When management assigns authorities and responsibilities to financial reporting positions, it considers the impact on the effectiveness of the control environment and the importance of maintaining effective segregation of duties.
- When delegating levels of authority and responsibility, management establishes an appropriate balance between the authority needed to "get the job done" and the need to maintain adequate internal control over key business processes.
- Employees are empowered to correct problems or implement improvements in their assigned business processes as deemed necessary. Empowerment to take these actions is accompanied by preapproved levels of responsibility and authority.
- Management considers the nature of employee positions within the organization when assigning responsibilities to individuals or determining certain levels of authority for positions.

Examples of Effective Ways to Achieve the Principle

Board Overseeing and Evaluating Certain Roles

The bylaws of a company's board of directors sets forth as one of the board's responsibilities the oversight and evaluation of the principal roles and responsibilities of key financial reporting management. To fulfill this responsibility, a representative of the board of directors meets with the company's human resource function, internal audit group leader, outside legal counsel, and external auditors to review certain members of management and the latest assessment of their roles and responsibilities.

In this forum, and in conjunction with an overall review of its organization chart and the respective responsibilities of each key position, the board of directors confirms that management has verified that key financial reporting roles and responsibilities are properly aligned with the expectations of the organization and the internal controls surrounding financial reporting. As a result of this discussion, the board of directors makes recommendations to management as to realignment of roles and responsibilities of key financial reporting management.

Management Assigning Levels of Authority

Management structured the finance department and assigned levels of authority and responsibility for specific positions. This was evidenced by the creation of a personnel organization chart depicting the assigned responsibilities at all levels and written job descriptions for all employees. Employees are evaluated based on the performance of those responsibilities.

Senior Management Reorganizing Reporting Lines

Senior management for a small, rapidly growing company realized that the assignment of roles and responsibilities for its management executives was no longer relevant. The CFO was performing certain roles that frequently were being duplicated by the controller. And, because information from the CEO was not being communicated clearly across the senior management team, the company lacked a clear direction for achieving its objectives. To strengthen its process of assigning authorities and responsibilities among its leadership team, the CEO initiated a project to define the authority and responsibility of each member of the senior management team, including finance and accounting management positions. As part of this redesign, the project team focused on segregation of duties, conflicts of interest, and the impact this restructuring would have on the overall control environment. Written job descriptions, which included specified authorities and responsibilities, were created for each senior management position. The result was a much clearer understanding of how the senior management function should operate to meet its financial reporting and other corporate objectives.

Properly Authorizing Material Transactions

A company established clear lines of authority for approval of transactions over specified dollar limits or meeting certain described characteristics (for example, involvement of a related party). As dollar thresholds increase, additional approvals from senior levels of management are required, with the highest dollar thresholds requiring CEO and board of director approval. All approvals are documented on prescribed forms.

Human Resources

Basic Principle

Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Attributes of the Principle

- *Establish Human Resource Policies* – Management establishes human resource policies and procedures that demonstrate its commitment to integrity, ethical behavior, and competence.
- *Recruiting and Retention* – Employee recruitment and retention for key financial reporting positions are guided by the principles of integrity and by the necessary competencies associated with the positions.
- *Adequate Training* – Management supports employees by providing access to the tools and training needed to perform their financial reporting roles.
- *Performance and Compensation* – Employee performance evaluations and the company's compensation practices, including those affecting top management, support the achievement of financial reporting objectives.

Approaches Smaller Companies Can Take to Achieve the Principle

- The company performs reference checks and reviews resumes in considering candidates for key financial reporting positions. For positions with greater authority and responsibility, the company also performs background checks.
- The company develops and maintains position descriptions that reflect its values and the competencies needed to execute position requirements.
- Human resource staff develop and periodically update an employee handbook outlining the company's human resource policies and procedures.
- The human resource function provides training and awareness programs to enforce and promote ethical behavior throughout the organization. Additional training programs are available to all employees, depending on their relative needs.
- An established review and appraisal process is in place to confirm awareness of each employee's progress and status within the organization.
- The company's process for performing exit interviews includes inquiries about any concerns related to the company's financial reporting and internal control.
- The company's compensation plan for senior executives includes a significant element tied to the achievement of nonfinancial goals (for example, customer satisfaction, and successful systems implementation) and is not excessively tied to short-term accounting results.

- The board reviews management compensation plans, including bonus and stock compensation components, to determine the extent that the plans increase the risk of financial reporting misstatements and implements additional controls to reduce those risks to an acceptable level (including modification of, or more direct oversight over, the compensation plans).

Examples of Effective Ways to Achieve the Principle

Developing Human Resource Practices

A company is not able to hire a full-time human resource person. As a result, it formed a task force comprising top management and other operating managers to develop human resource practices and policies. These policies, once developed, were reviewed and approved by the board, and were implemented by line management. The policies and procedures are documented and thus provide evidence of the control process. Further, any changes that occur in the policies and procedures are noted and signed off by appropriate personnel.

Periodically Reviewing Policies

A company periodically reviews its human resource policies and assesses the processes used to disseminate the policies throughout the organization and the level of understanding of those policies by all employees. The content, relevance, timeliness, and confirmation of understanding by employees are the primary focus of management's review and assessment. Newly hired employees receive the most current version of the company's policies and procedures upon starting their employment, and other employees receive updated policies when issued. Surveys are conducted periodically to assess whether employees are aware of the most recent versions of the company's human resource policies and procedures.

Periodically Assessing Objectives

A small company records all appraisal reviews of employees responsible for owning, executing, or testing controls related to the generation of financial reporting and disclosures. Employees' performances are documented against expectations established at the beginning of the year. This review takes the form of either a formal annual review process or more informal quarterly reviews of progress compared with objectives. In either event, the reviews are documented so that evidence of their occurrence can be retrieved. A follow-up email from the manager to the employee, with a copy to the human resource director, is an example of evidence.

Cross-Component Review

Documenting and Evaluating Entity-Wide Controls Using a Questionnaire

The CFO of a smaller software company (which has already filed its 404 report with the SEC) uses a questionnaire to assess the principles described in this guidance. The questionnaire is organized by principle and allows the company to systematically identify key entity-level controls and describes management processes for reviewing those controls. Appendix C includes a illustrative matrix.

Summary

Every business needs a sound control environment. Pressure is imposed on smaller public companies to have strong control structures. Management override in a smaller business can be controlled with a strong control environment along with the assistance of an active board and audit committee.

Small businesses, however, have a unique advantage in that they easily can establish a positive culture throughout the company. Typical smaller business management structures are transparent thereby enabling standards of integrity and ethics to be communicated to members throughout the company.

There may be initial incremental costs associated with strengthening a company's control environment, such as retaining independent board members. However the cost benefit of this investment can yield returns with prevention of potential fraud and errors.

4. RISK ASSESSMENT

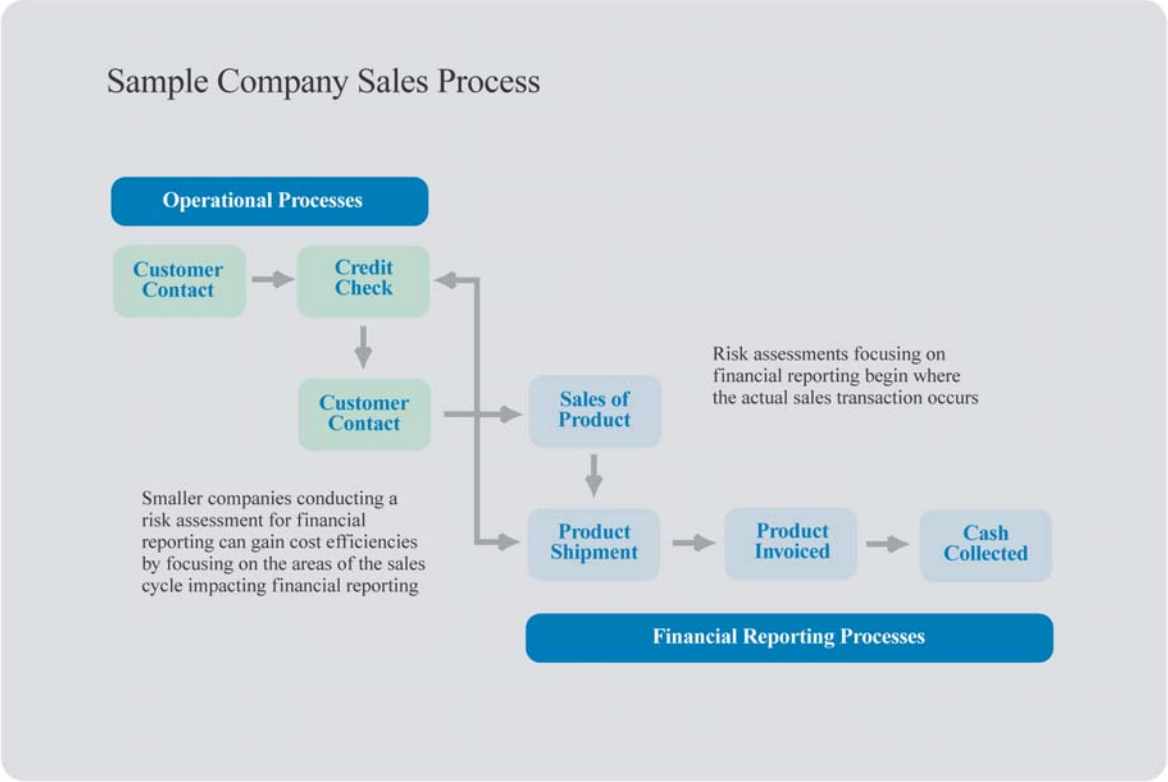
Companies set objectives and goals, and management identifies the risks to the achievement of those objectives. Controls then act to mitigate those risks. Financial reporting objectives address the preparation of reliable published financial information. The term "reliability" as used in the context of financial reporting objectives involves the preparation of financial statements that are fairly presented, in material respects, in conformity with generally accepted or other relevant and appropriate accounting principles and regulatory requirements for external purposes.

Risk assessment as it relates to the objective of reliable financial reporting involves the identification and analysis of the risks of material misstatement in those reports. The establishment of financial reporting objectives, articulated by a set of financial statement assertions, is a precondition to the risk assessment process.

This risk assessment process has traditionally has been informal and less structured in smaller entities than in larger ones, but approaches aligned to the basic concepts of this internal control component should be present in all companies. The process of identifying and analyzing risks that may prevent the achievement of financial reporting objectives often consists primarily of top management receiving information directly from employees and outsiders. Risk assessment in smaller companies can be particularly effective because the in-depth involvement of the CEO and other key managers often means that risks are assessed by people with both access to the appropriate information and a good understanding of its implications.

The output of the risk assessment process is important to the design and operation of control activities. In addition to potentially having fewer business processes and business units, smaller companies may be able to be benefit from being more specific in identifying risks resulting in the ability to tailor the control activities more precisely (that is, avoid unnecessary or unnecessarily redundant control activities). A thorough and well thought out risk assessment is a precursor to ensuring effective and efficient control activities.

A company developing its assessment will identify transactions and economic events that impact financial reporting and relate them to a specific process. Accordingly, management will need to separate process components that contribute to the overall profitability of the company's operations from transactional components that can impact financial reporting. As an example, the diagram on the following page illustrates a smaller company's revenue cycle. Reviewing initial parts of the process may identify operational improvements; however reviewing operational processes will likely incur greater effort and expense.



The focus of risk assessment in this chapter is on the identification and analysis of risks of material misstatement in financial reporting. Errors, irregularities, and misstatements might include:

- Not capturing all transactions
- Losing or altering items in the population of transactions
- Applying inappropriate accounting to transactions or estimates
- Inappropriately recording journal entries
- Recording transactions in the wrong period or at the wrong amount, or misclassifying transactions
- Failing to gather pertinent information to make reliable estimates
- Inappropriately applying formulas or calculations
- Misappropriation of assets
- Recording transactions that did not exist or did not occur.

Risk Assessment Principles

COSO has identified three major principles related to the achievement of control objectives at the risk assessment level. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section II of Appendix B.

8. ***Importance of Financial Reporting Objectives*** – A precondition to risk assessment is the establishment of objectives for reliable financial reporting.

9. ***Identification and Analysis of Financial Reporting Risks*** – The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.

10. ***Assessment of Fraud Risk*** – The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Importance of Financial Reporting Objectives

Basic Principle

A precondition to risk assessment is the establishment of objectives for reliable financial reporting.

Attributes of the Principle

- *Comply with Generally Accepted Accounting Principles* – Financial reporting objectives align with the requirements of generally accepted accounting principles.
- *Financial Statement Assertions*[5] – For each significant account and disclosure, financial reporting objectives are linked to a series of financial statement assertions that underlie a company's financial statements,[6] with some assertions more important/relevant depending on company circumstances.
  - *Existence* – Assets, liabilities, and ownership interests exist at a specific date, and recorded transactions represent events that actually occurred during a certain period.
  - *Completeness* – All transactions and other events and circumstances that occurred during a specific period, and should have been recognized in that period, have, in fact, been recorded.
  - *Rights and Obligations* – Assets are the rights, and liabilities are the obligations, of the entity at a given date.
  - *Valuation or Allocation* – Asset, liability, revenue, and expense components are recorded at appropriate amounts in conformity with relevant and appropriate accounting principles. Transactions are mathematically correct and appropriately summarized, and recorded in the entity's books and records.
  - *Presentation and Disclosure* – Items in the financial statements are properly described, sorted, and classified.
- *Materiality* – With respect to financial statement accounts and disclosures, significance is based on materiality and risk, considering both quantitative and qualitative factors. SEC Staff Accounting Bulletin (SAB) 99 requires companies to consider the context of the item and include important qualitative features as well as quantitative misstatements in determining whether an item is material. [7]

---

[6] Statement on Auditing Standards No. 31, AU Section 326, *Evidential Matter* (New York: AICPA, 1980). A set of assertions different from those listed may be used provided it encompasses all management representations that have a meaningful bearing on whether the significant financial statement accounts and disclosures are fairly stated.

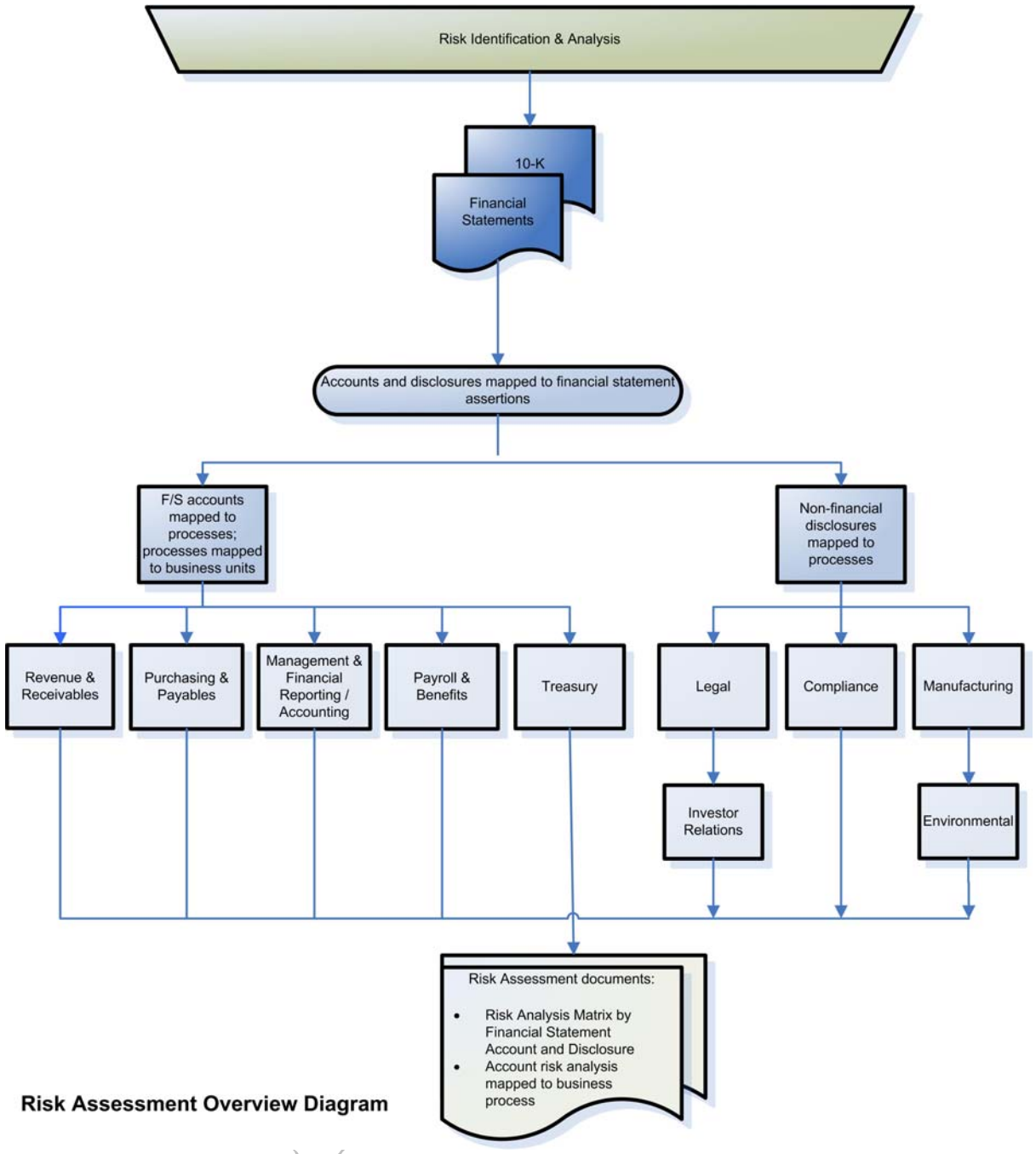
[7] Companies may want to consider SEC Staff Accounting Bulletin 99 and PCAOB Auditing Standard No. 2 *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*, when determining materiality and significance of accounts/processes with respect to internal controls.

Approach Smaller Companies Can Take to Achieve the Principle

- Management starts with the financial statements, including disclosures, and identifies financial statement assertions for each significant account and disclosure. Once the relevant financial statement assertions for each significant account and disclosure are identified, management identifies processes supporting these financial statement accounts.

Examples of Effective Ways to Achieve the Principle

Management begins its risk assessment process after establishing financial reporting objectives that address the preparation of reliable and relevant financial statements. The financial reporting objectives are supported by a series of assertions that underlie the company's financial statements. Assertions are linked to significant financial statement accounts and disclosures. Management determines significance of accounts and disclosures in conjunction with identifying and analyzing risks for each financial statement account and disclosure. This approach is diagrammed below.



Risk Assessment Overview Diagram

Identification and Analysis of Financial Reporting Risks

Basic Principle

The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.

Attributes of the Principle

- *Potential Risks* – Risks potentially impacting the achievement of financial reporting objectives are identified.
- *Include Business Processes* – Effective risk identification includes consideration of the business processes that impact financial statement accounts and disclosures.
- *Include Information Technology* – Information technology infrastructure and processes supporting the financial reporting objectives are included in the financial reporting risk assessment.
- *Internal and External Factors* – Risk identification considers both internal and external factors and their impact on the achievement of financial reporting objectives.
- *Involve Levels of Management* – The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- *Estimate Impact and Likelihood* – Identified risks are analyzed through a process that includes estimating the potential impact of the risk and an assessment of the likelihood of the risk occurring.
- *Triggers for Reassessment* – Management establishes triggers for reassessment of risks as changes occur that may impact financial reporting objectives.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company's risk identification process includes:
  - Mapping (linking) financial statement accounts and disclosures to business processes
  - Identifying and mapping information technology (IT) systems supporting key business processes relevant to financial reporting objectives
  - Mapping processes to business units.
- A company's risk identification considers interactions with relevant external parties that may affect the reliability of financial reporting. These external parties include potential and current suppliers, investors, creditors, shareholders, employees, customers, buyers, intermediaries, and competitors.
- A company considers external factors that impact its ability to achieve its financial reporting objectives, including, but not limited to, economic, competitive, and industry

conditions, regulatory and political environment, and changes in technology, supply sources, customer demands, or creditor requirements.

- A company considers internal factors that impact its ability to achieve its financial reporting objectives. These include account characteristics, business process characteristics, and entity-level factors.
- Risk analysis uses the following techniques:
  - Interviews with business process owners and other key personnel
  - Business process owners performing self-assessments of risks to financial reporting objectives in key business processes, with the results compiled and reviewed by key members of management
  - Meetings with appropriate levels of executive management.
- Management establishes criteria to assess the potential impact and likelihood of risks. The resulting assessment is used as a key input in determining required control activities.
- Risk assessments are updated on a quarterly basis, considering:
  - Newly identified risks determined to be significant
  - The escalation of previously identified risks to a higher priority
  - The status of action plans to mitigate prioritized risks.
- Management establishes specific risk identification and assessment processes in connection with significant internal and external changes affecting the business.
- Key finance personnel meet on a regular basis with information technology personnel to monitor changes in information technology that may affect risks related to financial reporting.
- Management meets with legal counsel at least quarterly in an effort to stay abreast of legal/regulatory changes.

Examples of Effective Ways to Achieve the Principle [8]

Analyzing Risks in Third-Party Operations

In analyzing its payroll and benefits cycle, a company identifies risks related to the completeness and accuracy of employee data maintained by its third-party payroll service provider. These risks include the risk of incomplete or inaccurate processing of data by the payroll administrator due to ineffective review and authorization controls, which could lead to errors in the financial reporting of compensation and benefit expenses. Additionally, the company identifies risks related to improper review controls, which could resulted in the set-up of fictitious employees, leading to further risks of fraudulent financial reporting.

Analyzing Risk Across Functions

A $20-million retailer with 75 employees and 10 retail stores convenes the department heads representing finance, human resources, merchandising, operations, and administration (management), and performs a risk analysis by functional department. Risks are rated from 1 to 5 (1 being the least risky and 5 the most risky) and are based on both significance to the business and likelihood of occurrence. The analysis is performed by discussion in a working session format, and the results are documented in a table that outlines the specific risk together with the rating and the factors that contribute to the rating. Risk identified related to revenue recognition is documented as follows:

- Revenue may not be recognized in accordance with GAAP.
- Risk rating = 5
- Factors contributing to risk rating:
  - Complexity of rules for revenue recognition
  - Knowledge level of people responsible for recording sales transactions
  - Complexity of promotion and discount transactions
  - Aggressive sales targets
  - Incentive and bonus structure
  - Supporting systems limitations

[8] A comprehensive risk assessment example is presented at the end of the chapter.

Analyzing Risk for Information Technology

In a $20 million dollar retailer with three information technology support personnel, application and general computer controls are driven by the critical applications identified that support the financial reporting process. This approach helps the company establish which information systems management will rely on. Prior to initiation of application and general computer controls design and implementation, the company takes the following three steps.

- Information technology management meets with the business process owners to review the results of the business process risk assessment. Information technology works to gain an understanding of how application data is utilized in the financial reporting process and determines whether there are other user controls (manual controls) in place that would mitigate the need for application and general computer controls.
- Information technology management creates a revised listing of critical applications that need to be addressed when designing application and general computer controls.
- Information technology management maps the critical applications to the operating systems, databases and information technology processes that support those applications. Packaged software and third party web applications typically reduce the number of information technology processes applicable to those applications.

Assessment of Fraud Risk

Basic Principle

The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Attributes of the Principle

- *Integral Part of Risk Assessment* – Fraud risk assessments are an integral part of the risk identification and analysis process.
- *Incentives and Pressures* – A company's assessment of fraud risks considers incentives and pressures, attitudes, and rationalizations, as well as opportunity to commit fraud.
- *Considers Risk Factors* – A company's assessment considers risk factors relevant to its industry and to the geographic regions where it does business.
- *Considers High-Risk Areas* – A company considers the potential for fraud in high-risk areas, including revenue recognition, management override, accounting estimates, significant unusual accounts, nonstandard journal entries, significant inter-company accounts, and vulnerabilities related to misappropriation of assets.
- *Audit Committee Oversight* – The audit committee understands and develops an independent conclusion on the effectiveness of management's fraud risk assessment processes. As indicated in the Control Environment chapter, the board of directors actively evaluates and monitors risks affecting the reliability of financial reporting, including the risk of management override.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company understands potential fraud indicators, which include incentives, pressures, opportunities, attitudes, and rationalizations, as a basis for conducting a fraud risk assessment.
- A company conducts regular fraud risk assessments by major balance sheet and income statement account for each location and division.
- A company conducts fraud risk assessments based on the type of fraud, namely, fraudulent financial reporting and misappropriation of assets.

Example of Effective Ways to Achieve the Principle [9]

Management of a 180-employee manufacturer of fiber optic components performs its fraud risk assessment based on the type of fraud. Management assesses risks related to the following areas for its single-location business unit:

- Financial fraud
- Theft of assets or services
- Misrepresentation
- Side letters or oral agreements on sales contracts with customers

The audit committee performs a review of management's assessment to determine the adequacy of antifraud controls.

Comprehensive Risk Assessment Example

The risk assessment process comprises principles that are interrelated. A company undertakes the identification of risks to the achievement of financial reporting objectives by considering the principles outlined above in the aggregate. Because the elements of risk assessment are not performed in discrete steps but are considered together, COSO believes the most meaningful illustration would include a comprehensive approach. Accordingly, the principles described above are interwoven into the comprehensive example below.

A multimillion-dollar software company develops, markets, and supports enterprise transaction management software. The company's family of products includes a package that tracks and analyzes electronic transactions. The company's corporate offices are located in Connecticut; it also operates business units in San Jose and St. Louis.

The risk analysis process considers a number of characteristics that include both quantitative and qualitative factors. In general, these characteristics are rated as "low," "medium," or "high" risk in relation to each financial statement account or disclosure. For quantitative factors there exist certain thresholds that define each risk category. For qualitative factors the risk rating is determined by management based on the attributes of each factor and its importance to each relevant financial statement account and disclosure.

In completing its risk assessment matrix, for each financial statement account and disclosure management performs an analysis of the following factors:

- *Impact on Financial Statements:* This is a quantitative measure of potential impact on financial reporting objectives. The financial statement account is assessed in relation to its respective category, such as total assets, revenues, operating expenses, and so

[9] A comprehensive risk assessment example is presented below.

forth. Accounts that are greater than 0% but less than 5% are deemed low risk, those greater than or equal to 5% but less than 10% are medium risk, and those greater than or equal to 10% are high risk.

- *Account Characteristics:* Management considers factors such as volume of transactions that are processed through the financial statement account/disclosure, judgment required, accounting complexity, changing rules/regulations that affect the account, and so on.
- *Business Process Characteristics:* Management identifies business processes that generate transactions in each of the financial statement accounts, considering factors such as complexity of the process, centralization of the process (in one or multiple locations), information technology systems that support the process, changes being made or new processes being added, and presence of external relationships within the process, such as with vendors, creditors, shareholders, customers, and competitors.
- *Fraud Risk:* Management conducts a fraud risk assessment by major balance sheet and income statement account. In conducting the fraud risk assessment, for each account management assesses the risk of misstatement due to fraudulent financial reporting and misappropriation of assets.
- *External Factors:* In assessing external risks for financial statement accounts and disclosures, management considers factors such as economic, competitive, and industry conditions, regulatory and political environment, and changes in technology, supply sources, customer demands, or creditor requirements.
- *Entity-Level Factors:* Management considers (internal) entity-level factors that could impact the company's ability to achieve its financial reporting objectives. These include, but are not limited to the nature of the company's activities and employee access to assets, the quality and quantity of personnel hired and the levels of training provided, disruptions in information systems processing or changes in information systems, and other organizational changes, including changes in key personnel or responsibilities. These entity-level factors are considered in relation to their effect on the internal factors assessed above, which include account characteristics, business process characteristics, and fraud risk.

Based on the above factors, overall risk ratings are established. Management uses these overall ratings to determine how each risk will be managed.

The risk assessment process described above is evidenced by the following risk matrices: Matrix 1 analyzes and rates the risks for each financial statement account and disclosure, together with the corresponding link to the relevant financial statement assertions (which support the financial reporting objective of reliable and relevant financial statements). Matrix 2 maps the accounts to business processes (excerpt of cash, accounts payable,

retained earnings, license revenue, and compensation expense). Matrix 3 addresses the company's information technology risk assessment by mapping critical business processes to the related information technology application and support infrastructure. This exercise represents the company's first steps in determining critical applications over which controls will need to be developed.

As part of the risk assessment process, the company also considers application and general computer controls in determining critical applications and mapping these to operating systems, databases, and information technology processes that support the applications.

The relevance of the financial reporting assertions reflects the overall rating. While all assertions are relevant for each financial statement account, certain assertions for higher risk accounts require greater attention than do similar assertions on lower risk accounts.

Risk Assessment Matrix 1

Risk Identification and Analysis by Significant Account and Disclosure

Financial Statement Account/Disclosure	As a % of Total	Impact on F/S	Account Charac-teristics	Business Process Charac-teristics	Fraud Risk	External Factors	Overall Rating	Relevant Assertions[10]				
								E/O	CO	V/A	R&O	P&D
BALANCE SHEET												
Assets												
Cash & Cash Equivalents	6%	M	H	M	H	H	H	✓	✓		✓	✓
Accounts Receivable	30%	H	H	H	H	H	H	✓	✓	✓		✓
Prepaid Expenses	4%	L	M	L	L	L	L	✓		✓		
Inventory	35%	H	M	M	L	L	M	✓	✓	✓	✓	✓
Property & Equipment	15%	H	L	L	L	L	L	✓		✓	✓	
Intangible Assets	10%	M	M	M	M	M	M	✓		✓	✓	✓
Liabilities												
Accounts Payable	35%	H	H	L	M	M	M	✓	✓		✓	
Accrued Expenses	20%	H	M	M	H	H	H	✓	✓	✓	✓	✓
Deferred Revenue	30%	H	M	M	M	L	L	✓	✓	✓	✓	✓
Long-Term Debt	15%	H	L	L	L	H	L	✓	✓	✓	✓	✓
Shareholders' Equity												
Common Stock	5%	M	M	M	L	L	L	✓		✓	✓	✓
Retained Earnings	95%	H	L	L	L	M	H	✓	✓			✓

[10] E/O – Existence/Occurrence
CO – Completeness
V/A – Valuation/Allocation
R&O – Rights & Obligations
P&D – Presentation & Disclosure

Financial Statement Account/Disclosure	As a % of Total	Impact on F/S	Account Charac-teristics	Business Process Charac-teristics	Fraud Risk	External Factors	Overall Rating	Relevant Assertions[10]				
								E/O	C O	V / A	R & O	P & D
INCOME STATEMENT												
Revenues	-											
Product License Revenue		H	H	H	H	H	H	✓	✓	✓		✓
Professional Services Revenue		H	H	M	M	H	H	✓	✓	✓		✓
Cost of Goods Sold	60%[11]											
Cost of Software License		H	H	H	H	H	H	✓	✓	✓		✓
Cost of Professional Services		H	H	M	M	H	H	✓	✓	✓		✓
Operating Expenses	20%											
Compensation & Related Benefits		H	H	H	M	H	H		✓	✓		✓
Marketing & Selling Expenses	10%	M	M	L	L	L	M		✓	✓		✓
R&D Expenses		M	L	L	L	M	L					
G&A Expense		M	M	L	L	L	M		✓	✓		✓
Depreciation & Amortization		M	M	M	L	L	M		✓	✓		✓
Other Income/ Expense	5%											
Interest Income/ (Expense)		L	L	M	L	M	M	✓	✓			✓
Income Taxes		L	M	H	M	H	H		✓	✓		✓

Note: **The** Presentation and Disclosure financial statement assertion is relevant to all accounts and classes of transactions; however, for the most part, this assertion is assessed at the overall financial statement level in the context of the financial reporting business process.

Risk Rating

H – High; M – Medium; L – Low

[11] Expressed as a percentage of revenue

Risk Assessment Matrix 2

Mapping of Account Risk Analysis to Business Process[12]

	Account Name	Cash & Cash Equivalents	Accounts Payable	Retained Earnings	License Revenue	Compensa-tion Expense
	Overall Rating	**H**	**M**	**H**	**H**	**H**
Treasury	Cash Management	H	M	H	H	H
	Investment Securities	H				
Revenue & Receivables	Order Management					
	Credit & Collections	H			H	
	Revenue Recognition				H	
Purchasing & Payable	Purchasing to Payables		M		H	
	A/P and Cash Disbursements	H	M			H
Payroll & Employee Benefits	Employee Master File Maintenance					H
	Payroll Management & Benefits	H				H
	Incentive Compensation	H				H
Equity	Stock Administration & Equity Transaction	H		M		
Taxes	Income Tax Provision & Compliance	H				
GL Closing & Reporting	Manage GL and Closing	H	M	M	H	H
	Consolidation	H	M	M	H	H
	External Reporting & F/S Disclosure	H	M	M	H	H

[12] This matrix is an excerpt of the complete matrix completed by the company.

Risk Assessment Matrix 3

Map Critical Business Process to Critical Application and Support Infrastructure

Business Processes and Sub-processes	Overall Rating	Application Name	Database	Operating System	Critical Spreadsheet Name	Supported by a Third Party	Hosted by a Third Party Provider
Cash Management	H	Treasury Management Software	Embedded	Windows	N/A	No	No
Investment Securities	H	Spreadsheet	N/A	Windows	Spreadsheet	No	No
Order Management	H	Financial Software	Proprietary Database	UNIX	N/A	Yes	Yes
Credit and Collections	H	None	N/A	N/A	N/A	N/A	N/A
Revenue Recognition	H	Financial Software	N/A	N/A	Spreadsheet	N/A	N/A
Purchasing to Payables	H	Financial Software	Proprietary Database	Windows	N/A	Yes	Yes
A/P and Cash Disbursements	H	Financial Software	Proprietary Database	Windows	N/A	Yes	Yes
Employee Master File Maintenance	M	Payroll Software	Embedded	UNIX	N/A	Yes	Yes
Payroll Management & Benefits	H	Payroll Software	Embedded	Windows PC Based	Employee Benefits, Time Sheets	Yes	Yes
Incentive Compensation	M	Spreadsheet	N/A	Network File Shares	Incentives	No	No
Stock Administration & Equity Transaction	M	Stock Option Software	Embedded	Windows PC Based	N/A	Yes	Yes
Income Tax Provision and Compliance	H	Income Tax Software	Embedded	Windows	N/A	No	No
Manage GL and Closing	H	Financial Software	Proprietary Database	Windows	N/A	Yes	Yes
Consolidation	H	Spreadsheet	N/A	Windows	Financial Spreadsheets	No	No
External Reporting & F/S Disclosure	H	Word Processing	N/A	Windows	N/A	No	No

When assessing the extent of required documentation, management bases its decision on the following risk ratings:

- *High* – These are critical processes that require process documentation, including a risk/controls matrix to describe key risks and the controls that mitigate those risks. Process maps and narratives also are developed to describe the flow of transactions within the process and to identify the control points. Controls are identified as preventive or detective; and whether manual or system based. Policies and procedures also are developed that help guide employees and control activities.
- *Medium* – These are processes for which management prepares process documentation that includes a risk/controls matrix to describe key risks and controls that mitigate those risks. Process maps and narratives are developed where applicable at a high level. Policies and procedures are developed, but may be less formally documented.
- *Low* – These are processes that require minimal process documentation. The extent of documentation may cover policy/procedures and applicable controls.

The company updates the risk assessment frameworks developed above through ongoing monitoring of risk in the business (internal factors that include account and business process characteristics) and the business environment (external factors). As an example, information technology managers meet with key finance personnel monthly to discuss process/changes/projects in each functional area of the information system that relates to financial reporting. These meetings are used to update team members and discuss issues or changes to the company's processes. The changes are evaluated within the same risk identification and analysis process as outlined above to determine each additional risk's significance in the context of the previous risk prioritization. Additionally the company meets with its legal counsel quarterly to discuss effects of any external regulatory changes that may impact financial reporting.

Summary

Organizations establish financial reporting objectives and goals, which are generally articulated by a set of financial statement assertions. Management implements processes to identify risks that threaten the achievement of those financial reporting objectives and implements responses to mitigate those risk. Thus, risk assessment is a precondition to identifying internal control responses to identified risks.

Risk assessment identifies and analyzes risks that could result in material misstatements in the company's financial reporting. Smaller companies will likely adopt processes that are similar in approach to those of their larger counterparts, but on a smaller scale.

To manage incremental costs, smaller business, like their larger counterparts, can focus their risk assessment efforts on identifying the stages in a transaction cycle that potentially impact financial reporting and the supporting financial applications. Information obtained by management about risks within those transaction processes is important to the design and operation of control activities within those processes. Control activities can be tailored to the entity to ensure effective and efficient control activities.

5. CONTROL ACTIVITIES

Control activities are performed at various levels of the company to reduce risks to the achievement of financial reporting objectives. At higher levels, management performs top-level reviews comparing actual performance to budget and forecast, reviews financial reports, and considers performance indicators relating different operational and financial information. Wider spans of control allow management of smaller businesses to effectively use these types of reports to manage the business – detecting potential deficiencies in the operation of process-level control activities and changes in operations that may warrant attention. For this reason, some management control activities serve as both a control activity and a monitoring activity, and users may wish to consider the guidance in the Monitoring chapter when evaluating the overall effectiveness of the company's control activities.

At lower levels in the company, staff develops and deploys policies and procedures related to financial processes to effectively capture information in the company's accounts. Many smaller companies also develop and deploy compensating controls where resource constraints compromise the ability to segregate duties. Management also establishes information technology controls as needed to support financial reporting objectives.

Control activities in smaller companies reflect their organizational characteristics, which include greater concentration of decision-making authority, wider spans of control, and more direct channels of communication. As an example, management frequently communicates directives orally to employees. Smaller entities can achieve effective control over financial reporting through a combination of controls that includes oversight controls applied by management, and can prepare and maintain a level of documentation that allows for the effective transition of job responsibilities.

Many companies attain insight into the effectiveness of their controls through interaction with outside entities including suppliers, contractors, and customers. However, such feedback is not provided regarding adjusting entries, the closing process, or accounting estimates. Consequently, many accounting frauds – in both large and smaller companies – have been perpetrated by manipulating accounting estimates or closing entries. Smaller businesses must develop effective oversight over such entries. The oversight can come in the form of summary reports on adjusting entries that are presented to management on a periodic basis. Summary reports also can be developed that compare accounting estimates in the current period with prior periods and, more importantly, with other companies in the industry, where available, and with changes taking place in the economic environment. The board or management also may wish to have someone objective review the assumptions underlying estimates.

Control Activity Principles

COSO has identified four major principles related to the achievement of control objectives at the control activities level. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section III of Appendix B.

11. ***Elements of a Control Activity*** – Policies and procedures are established and communicated throughout the company, at all levels and across all functions, that enable management directives to be carried out.

12. ***Control Activities Linked to Risk Assessment*** – Actions are taken to address risks to the achievement of financial reporting objectives.

13. ***Selection and Development of Control Activities*** – Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives.

14. ***Information Technology*** – Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Elements of a Control Activity

Basic Principle

Policies and procedures are established and communicated throughout the company, at all levels and across all functions, that enable management directives to be carried out.

Attributes of the Principle

- *Policies and Procedures* – Control activities involve two elements: (1) a policy establishing what should be done and (2) procedures to accomplish the policy. Policies specify what is allowable or should be done to mitigate specific risks. Procedures specify how the action prescribed is performed, including the parameters of acceptable performance.

- *Cascade into the Company* – Control activities reflecting board-level policies permeate from the board into the company's functions, departments, and processes.
- *Criteria for Accomplishment* – Management establishes the criteria for determining the parameters that define "accomplishment" of the policy objectives, that is, the criteria relate to the level of processing that sufficiently mitigates risks.
- *Monitored* – Policies and procedures of the company are monitored and immediate corrective actions are taken for exceptions that are not within established tolerances.
- *Track Implementation* – Procedures are designed such that management can track the implementation and effectiveness of actions taken to manage risks relevant to financial reporting objectives.
- *Documented* – Policies and procedures that are critical to the accomplishment of financial reporting objectives, as determined from the risk assessment process, are documented, and that documentation is made available to staff as necessary.
- *Ownership* – Ownership of policies and procedures resides with the management of the business or function in which the relevant risk resides.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company develops board-level policies for areas that have entity-wide application, such as its code of conduct, privacy, delegation of authority, safeguarding of assets, and so forth.
- A company develops and documents policies and procedures for all significant financial reporting activities and other significant functional areas using various formats, such as narratives, flowcharts, and matrices.
- Management communicates key policies and related procedures to staff using printed material filed in binders or electronic documents retained on a shared network or on an intranet to which employees are directed.

- A company develops a standardized template for documenting its policies. This template includes:
  - Reason or purpose for the policy
  - Scope of the policy
  - Locations to which the policy applies
  - Roles and responsibilities for ownership, creation, implementation, and maintenance of the policy
  - Key provisions covered by the policy.
- A company's policies define what should be done. The actions then become the procedures, which are documented in a matrix, thereby evidencing the basis of the company's controls.

Examples of Effective Ways to Achieve the Principle

Using Templates to Document Policies

A company uses a standardized template to document policies. Its credit and collection policy addresses:

- *Reason* – outlines the policy for the credit application and approval process used to extend trade credit to the company's customers.
- *Scope* – outlines the parameters and areas to which the policy applies, that is, all trade customers within the contiguous United States.
- *Location* – specifies the policy's geographic boundaries – that it applies company-wide across all regions and business units.
- *Roles and Responsibilities* – outline the roles/responsibilities of all those involved in the credit application and approval process. This includes the sales representative (files the credit application), credit analyst (performs the credit check and recommends a credit limit), controller (reviews the credit check and approves the credit limit), and customer service manager (enters the credit limit into the customer file).
- *Key Provisions* – address credit approval policy with respect to the responsibilities of all those involved in the credit application process; cover steps from credit application initiation through credit checks and approval for credit and credit limit.

Documenting and Approving Key Business Processes

A company formally documents policies for its key business processes in the form of policy statements, which are approved by the board and communicated to employees through the company intranet. These policy statements deal with spending authority, revenue recognition, purchase orders (expenditure requisitions), code of conduct, whistleblowers, and fixed asset acquisitions, depreciation, and disposition. For other processes whose risks are deemed to be noncritical but important (as assessed during the risk analysis process), such as invoicing, distribution, and collections, the company documents procedures and controls within the risk/controls matrix.

Board-Level Policies for Safeguarding Assets

A company sets a board-level policy governing the board's stewardship over the safeguarding of assets. At the corporate level, this further states that management establishes internal controls to provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements. From this, the information technology department develops policies and supporting procedures guiding staff use of company computers; the controller's department develops policies and supporting procedures guiding cash management; and the purchasing department develops policies and procedures for access to parts inventory.

Policies for Cash Disbursements

A company establishes a policy that all payments must be appropriately authorized before cash is remitted. This policy applies at all levels of the company, with approval limits set in relation to the authority of the individual or group. The policy establishes that a payables clerk may approve cash payments up to $500; the controller, $2,500; the CFO, $20,000; and the CEO, $100,000. All transactions involving cash payments exceeding $100,000 must be approved by the board.

Control Activities Linked to Risk Assessment

Basic Principle

Actions are taken to address risks to the achievement of financial reporting objectives.

Attributes of the Principle

- *Integrated into Business Processes* – Control activities are built into the company's regular business processes and the day-to-day activities of its employees.
- *Include All Significant Points of Entry into the Company's General Ledger* – Control activities include controls related to all aspects of the recording process, including adjusting and closing journal entries and accounting estimates.
- *Mitigate Risks* – Control activities are designed to mitigate risks impacting financial reporting objectives.
- *Risk Based* – The selection of control activities is based on the risk assessment process, emphasizing processes and also classes of transactions, and financial statement accounts and disclosures that could contain misstatements that individually, or in the aggregate, could have a material impact on the company's financial statements.
- *Encompass Information Technology* – The selection of control activities encompasses relevant information technology controls.
- *Continued Relevance* – Policies and procedures are reviewed periodically by management to determine their continued relevance.

Approaches Smaller Companies Can Take to Achieve the Principle

- Many companies focus their review of control activities on detailed processes that impact financial reporting. Alternatively, a company can first look at its entity-level controls that are pervasive across the company. Doing this in combination with a risk assessment allows management to make a more informed decision as to which detailed processes need additional review, and the depth of that review. In determining the depth of review, management also considers the requisite blend of control activities and ongoing monitoring activities.
- A company uses process maps, narratives, spreadsheets, or other mechanisms to document and communicate needed control activities.
- A company outsources some of its operations to a third party and has a contract with the third party regarding controls over reports back to the company, including independent assessment of the reliability of the reports.
- A company uses facilitated workshops or self-assessment mechanisms to identify needed control activities for each identified risk to a financial reporting objective and as a means for training its employees regarding the proper implementation of control activities.

- A company utilizes a software tool that provides an inventory of potential controls aligned to potential risks to financial reporting, including a pre-populated inventory of common controls by business process. This facilitates the monitoring, updating, and testing of control activities.
- When outsourcing all or a portion of its financial reporting function, a company either obtains a SAS 70 Type II report or undertakes procedures to assess controls in place for the initiation, recording, and processing of significant classes of transactions at the third-party outsourcer.

Examples of Effective Ways to Achieve the Principle

Focusing on Account Estimates and Adjusting Entry Risks and Controls

A property management company developed, in conjunction with its risk assessment process, a spreadsheet setting out the financial reporting objectives and assertions, identified risks, and control activities intended to mitigate each risk. This entity-level review considered tasks such as general ledger maintenance, accruals, management estimates and reserves, goodwill and other intangible assets, period-close procedures, consolidation, financial statement preparation, and regulatory filings and disclosures. Management reviewed the type of control activity (preventive versus detective, manual versus automated, and other criteria) to determine the overall adequacy of the control activities in reducing risks to the financial reporting objectives. This spreadsheet provides evidence that the company linked its control activities to its risk assessment process. The controls are described in sufficient detail to allow management and others to evaluate the effectiveness of their design. Appendix C contains a sample listing of certain accounting estimates and adjusting entry risks and controls.

Using Templates of Common Control Activities

A small software developer acquired a template of common control activities, with supporting forms, relating to the hiring process. This template also includes reference to relevant laws and regulations potentially impacting the company. Management reviewed the summary of potential control activities and linked these to the risks identified in its earlier risk assessment to develop policies and procedures appropriate to its business. In addition, the company reviewed the template of common control activities to identify any potential risks not previously noted, and added those control activities considered necessary. The template is retained as evidence that the process design is linked to the risk assessment findings.

Control Activities for Outsourcing Activities Where a SAS 70 Report Is Available

A small public bio-tech company utilizes a third-party service organization as its transfer agent to oversee shareholder servicing needs. The third-party transfer agent is a registered transfer agent with the Securities and Exchange Commission. To assess whether transactions are initiated, processed, and recorded appropriately and physical safeguards and data access controls are in place, the transfer agent engages a service auditor to report on controls placed in within its transfer agent applications and tests those controls operation effectively (following procedures prescribed by the AICPA in Statement on Auditing Standards 70). This type of report is commonly is referred to as a SAS 70 Type II report. The company obtains the service auditors report and considers the following with respect to user controls:

- Controls exist around the review and authorization of data sent to the transfer agent and these are in compliance with the provisions of the servicing agreement between the transfer agent and the company.
- Controls are in place and operating effectively at the company over access to the transfer agent systems.
- Notification/instructions to the transfer agent for changes to stock issuance are authorized by the appropriate principals at the company.
- Relevant corporate actions are communicated to the transfer agent on a timely basis.
- Controls exist within the company for the receipt of information from the transfer agent and for the recording of transactions based on this information.

The following exhibit presents an example of how a company might approach the documentation and evaluation of control activities. Exhibit 5.1 is a flowchart developed by a small business utilizing "off the shelf" software. The flowchart and accompanying comments provide documentation of the controls. The flowchart has several other advantages:

- The nature of the control procedures performed is clearly documented.
- Responsibilities for the processing and control procedures are documented.
- Management has one flowchart it can use to evaluate the risks and the adequacy of related controls.
- The documentation of the controls provides a basis for testing their effectiveness.

Many smaller businesses use spreadsheets or similar technology to prepare or generate comprehensive matrices or other documentation of internal control over financial reporting processes. The use of such a matrix has the following advantages:

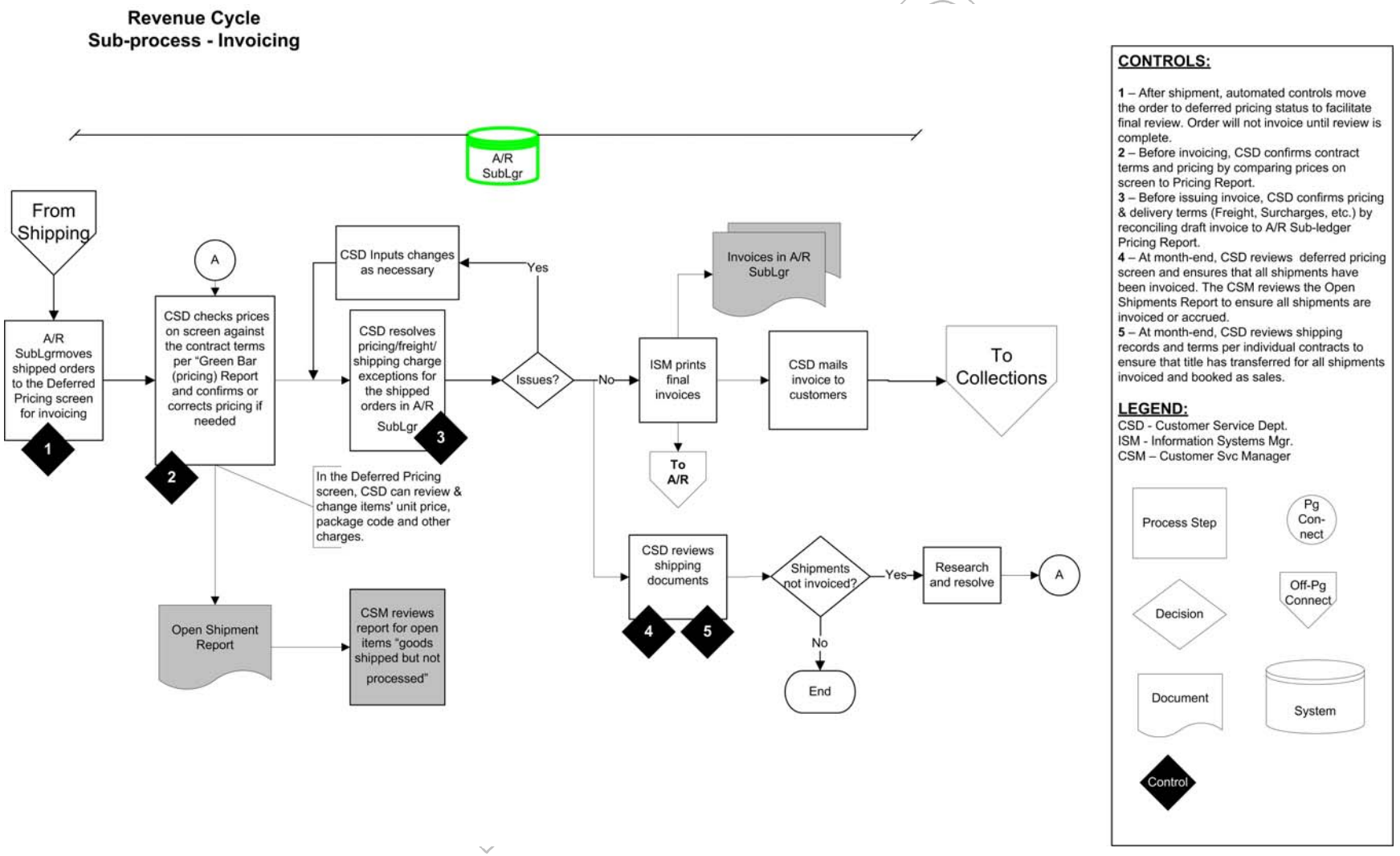
- The processing and related control procedures are clearly defined.
- The related financial statement assertions.

- The control objectives and control procedures are clearly linked to the risks that are mitigated.
- The nature of the control is clearly articulated (manual or automated, preventive or detective).
- The descriptions of the controls present a focal point for determining (a) which controls need to be tested, (b) how they might be tested, and (c) results of actual testing.
- The descriptions provide built-in documentation of the controls.

This documentation helps management form an overall assessment of the adequacy of internal control over financial reporting. There is also an opportunity to identify control deficiencies in a timely manner so that corrective action, or addition of needed procedures, can be addressed in a timely and cost-effective manner.

Our review of smaller companies, as well as of many larger companies, indicates that many companies utilize the matrix approach to document and evaluate their internal controls. Appendix D presents an illustrative matrix as an example of a template a company could use to document and evaluate the effectiveness of internal control over financial reporting. Many companies also add others column, such as those detailing the nature and level of unmitigated risks if the control design is not adequate to sufficiently mitigate the risk associated with the processing or the person(s) responsible for the control.

Exhibit 5.1


Revenue Cycle
Sub-process - Invoicing
A/R SubLgr
From Shipping
A/R SubLgrmoves shipped orders to the Deferred Pricing screen for invoicing
1
A
CSD checks prices on screen against the contract terms per "Green Bar (pricing) Report and confirms or corrects pricing if needed
2
CSD Inputs changes as necessary
Yes
CSD resolves pricing/freight/ shipping charge exceptions for the shipped orders in A/R SubLgr
3
In the Deferred Pricing screen, CSD can review & change items' unit price, package code and other charges.
Issues?
No
Invoices in A/R SubLgr
ISM prints final invoices
CSD mails invoice to customers
To Collections
To A/R
Open Shipment Report
CSM reviews report for open items "goods shipped but not processed"
CSD reviews shipping documents
4
5
Shipments not invoiced?
Yes
Research and resolve
A
No
End
CONTROLS:
1 – After shipment, automated controls move the order to deferred pricing status to facilitate final review. Order will not invoice until review is complete.
2 – Before invoicing, CSD confirms contract terms and pricing by comparing prices on screen to Pricing Report.
3 – Before issuing invoice, CSD confirms pricing & delivery terms (Freight, Surcharges, etc.) by reconciling draft invoice to A/R Sub-ledger Pricing Report.
4 – At month-end, CSD reviews deferred pricing screen and ensures that all shipments have been invoiced. The CSM reviews the Open Shipments Report to ensure all shipments are invoiced or accrued.
5 – At month-end, CSD reviews shipping records and terms per individual contracts to ensure that title has transferred for all shipments invoiced and booked as sales.
LEGEND:
CSD - Customer Service Dept.
ISM - Information Systems Mgr.
CSM – Customer Svc Manager
Process Step
Pg Con-nect
Decision
Off-Pg Connect
Document
System
Control

Selection and Development of Control Activities

Basic Principle

Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives.

Attributes of the Principle

- *Range of Activities* – Control activities include a range of activities that vary in terms of cost and effectiveness, depending on the circumstances. These include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
- *Preventive and Detective* – Management uses an appropriate balance of preventive and detective controls, and an appropriate balance of manual and automated controls, to mitigate risks to the achievement of financial reporting objectives.
- *Segregation of Duties* – Within the constraints of available resources, duties are logically divided among people or processes to mitigate risks and meet financial reporting objectives.
- *Compensating Controls* – Management uses compensating controls to counterbalance the potential effect of an internal control weakness and therefore reduce risk of financial misstatement to a relatively low level.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company uses risk/control matrices developed in the process of assessing risks and designing controls to perform a "gap analysis" to evaluate the need for additional controls to mitigate risks to the achievement of financial reporting objectives relating to each business process. The company then designs a mix of manual and/or information technology-based controls that are preventive or detective, as appropriate.
- A company assesses the costs of addressing identified risks using various control mechanisms, and weighs the costs against potential effectiveness of the controls in mitigating the respective risks. The company focuses on designing controls that are cost effective, but also confirms that the set of controls, taken together, provides reasonable assurance that risks to the achievement of financial reporting objectives relating to each process are mitigated.
- A company uses organization charts or similar documentation of activities, which it updates regularly to reflect current responsibilities and activities. This documentation is reviewed periodically by management to identify incompatibilities in functions and maintain segregation of duties.
- Where resource constraints compromise the ability to segregate duties to achieve financial reporting objectives effectively, management considers compensating control

activities, such as periodic management reviews of reports prepared in sufficient detail and in a timely fashion to facilitate identification of misstatements.

- A company separates incompatible activities by assigning them to different personnel or, in some cases, through implementation of information technology applications. Information technology, for example, is used to restrict access to data or programs, thereby enhancing segregation of duties. The company also uses software systems that report all unauthorized access to data or programs.
- A company uses the assertion approach for account balances, transactions, and disclosures to identify relevant controls to achieve the assertion and mitigate risk of misstatement.
- In a smaller company where limiting access to accounting records is not practical, management, process owners, or the internal auditors monitor those records closely for potential misstatements.

Examples of Effective Ways to Achieve the Principle

Segregating Cash Payments

A smaller company determined the need to segregate access to cash payments from the record-keeping process. With only a few office employees, management decided that all checks would require two manual signatures, so both the CEO and CFO sign the checks. The person preparing the checks was not granted signing authority. A similar company with the same challenge implemented software that prints electronic signatures on checks. The CEO and CFO are required to review pending payments in the system and to approve them before the checks are produced. The person preparing the checks cannot approve payments.

Compensating Controls over Inventory

A small furniture manufacturer stores supplies in a locked storeroom. The storeroom contains the materials and supplies used in constructing, repairing, and refinishing furnishings. The company lacks segregation between access to the storeroom and related accounting records, reducing the effectiveness of controls that help protect the inventory from loss or misappropriation. One individual has the responsibility for submitting purchase requests and receiving, issuing, and recording materials and supplies. Additionally, the same individual has the capability to delete and change transactions in the automated inventory system. Because there are limited controls to ensure that all purchases have been recorded and no transactions have been changed, materials and supplies could be lost or misappropriated without detection.

The company has used a compensating control to check the above balances because it does not have sufficient staff resources to separate these functions. Materials and supplies are spot checked periodically and reconciled to purchase orders maintained by the purchasing manager. Also, the capability to delete and change transactions has been limited to

individuals outside of the storeroom. These compensating controls provide reasonable assurance that items purchased were properly entered into the inventory system and that inventory balances are accurate.

Compensating Controls over Purchases

A smaller retail plumbing supply company has only two staff in its purchasing department. Both individuals are authorized to prepare purchase orders up to $5,000. As these purchase orders are not reviewed prior to being sent to vendors, the company has higher risk that unintentional errors or intentional acts will result in inventory valuation errors, obsolescence, or existence errors from diverted shipments. To reduce the level of risk to an acceptable level, management relies on a combination of actions of other staff, including the:

- Inventory receiving clerk who considers unusual inventory movement, such as excessive ordering that could lead to obsolescence
- Inventory clerk, who considers overall inventory levels, also reduces the risk of obsolescence
- Payables clerk, who matches payable invoices to purchase orders and receiving reports before amounts are paid, reduces the risk of existence errors resulting from diverted shipments
- Controller, who reviews exception reports of all inventory purchases with a price more than 15% above current average costing.

Taken together, these other controls result in management assessing the level of risk from the initial weakness in procurement as acceptable

Compensating Controls over Fixed Assets

A smaller high-tech company had considerable fixed assets, mostly in the form of personal computer and network equipment. Fixed asset acquisitions, retirements and disposals were approved by the controller. The staff accountant recorded these acquisitions, retirements and disposals in the general ledger and the supporting schedules maintained in spreadsheets (property ledger). The staff accountant also reconciled the property ledger to the general ledger, giving the staff accountant access to both the recording and reconciling functions. As part of the overall monitoring activities, the controller reviewed this reconciliation.

As a compensating control to reduce the risk from this lack of segregation, the controller prepares, on a monthly basis a management report for review by the CEO and CFO. The management report package included a budget to actual of capital expenditures and details of retirements and disposals that the top management team (consisting of four people) could review and query. A combination of the monitoring and compensating control helped mitigate the risk of error resulting from the lack of segregation.

Preventive and Detective Controls to Safeguard Assets

A small mining/refining company has quantities of gold in its warehouse. The company developed three levels of defense against unauthorized access to the gold inventory. First, as a preventive control, the gold is stored in a locked vault with only the refining manager and production manager having access to the vault. Two combinations are required to open the vault. Second, also as a preventive control, the vault is located in a separate room used only to pour and store the gold. Access to the room is restricted to the mine manager, production manager, mill manager, and mine security. Third, as a detective control, all gold added to or removed from the vault is weighed and logged. The log is stored in a separate part of the gold room. To detect any variations, the gold is weighed and reconciled to the log on a weekly basis, at the end of each financial reporting period, and before any shipment of gold from the mine.

Balancing Cost and Effectiveness

A small builder of inflatable boats maintains only a minimal amount of inventory on hand at the end of any quarter, and inventory turns every 45 days. The company has a simple accounting system in place that tracks inventory purchases and reallocates costs to finished goods as each boat is completed. As part of the company's risk assessment process, management reviews the risks within the inventory process and the potential impact on reliability of financial reporting. The company considered developing more rigorous controls over inventory, including regular and comprehensive cycle counts. Alternatively, the company considered whether limited cycle counts each quarter would be an effective means for mitigating the risk that inventory quantities in the system do not reflect inventory quantities on hand. The company concluded that a limited number of counts performed quarterly would reduce the risk of errors in its quarterly financial statements to an acceptable level.

Information Technology

Basic Principle

Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Attributes of the Principle

- *Application Controls* – Application controls are:
  - Built into computer programs and supporting manual procedures
  - Designed to provide completeness and accuracy of information processing critical to the integrity of the financial reporting process, authorization, and validity.
- *General Computer Controls* – General computer controls are broad and include controls over access, change and incident management, systems development and deployment, data backup and recovery, third party vendor management, and physical security critical to the integrity of the financial reporting process.
- *End-User Computing* – End-user computing processes, including spreadsheets and other user-developed programs, are documented, secured, backed up, and regularly reviewed for processing integrity.

Approaches

When considering the approaches that a company can take to achieve the principle, it is important to note that the design and implementation of information technology controls are directly related to those critical application, databases and systems identified during the risk assessment process outlined in the *Risk Assessment* chapter.

Several factors influence the level of required general computer controls and application controls in a smaller business. For instance, a smaller business that uses packaged software products for which source code cannot be modified, and that has limited Internet connectivity, will have a reduced level of general computer controls such as access controls, change and incident management controls, and systems development and deployment controls. Conversely, a company that has in-house-developed programs or applications developed by a local technology vendor, and has access to the source code, will require an expanded array of general computer controls and application controls.

Following are approaches and examples tailored to each of these computer environments.

Approaches Smaller Companies with Packaged Software Can Take to Achieve the Principle

Concerning the company's infrastructure, management:

- Secures access to critical applications, databases, operating systems, and networks. For instance:

- Access controls are implemented that identify who should have access to financial data and related programs. Account set-up, change and termination standards are followed.
- Authentication controls are established including a policy regarding the minimum requirements for unique user ID's and password standards. Exceptions are approved by senior management.
- Processes are monitored to confirm access rights.
- Parameters for restricting external connectivity to the system via such mechanisms as firewalls, VPN connections, and dial-up are reviewed.
- Access to powerful system ID's (e.g. super users, root, etc) for critical applications, databases, operating systems, and network devices is set by policy and assigned to personnel that need to have access to those IDs. Approval is obtained from the appropriate level of management and access is reviewed and monitored.
- Anti-virus software is used protect the integrity and security of financial reporting systems and subsystems. Processes are in place to maintain current anti-virus versions.

- Develops change and incident management processes. While the underlying code or data in packaged applications does not change significantly, the operating system that the application resides on changes periodically. Additionally, significant upgrades to packaged applications are issued from time to time and need to be implemented. These upgrades are subjected to a change management control process. The number of change management incidents will occur less often with packaged applications than with internally developed and supported software. For instance:
  - Change management policies and procedures define what changes require documentation and what changes do not. Significant changes to operating systems are initiated, approved and tracked.
  - For significant software vendor upgrades or changes related to critical information technology support infrastructure, all significant changes are tested prior to release into production. The level of detailed testing depends on the complexity and risk of the change to critical financial systems.
  - Detailed back-out plans exist for changes that cannot be performed in a segregated, controlled environment.
  - Where emergency changes are made to critical financial systems:
    - An audit trail exists for of all emergency activity as is independently reviewed.
    - Changes are supported by appropriate documentation.
    - Back-out procedures exist.
    - Changes are tested and subject to standard approval procedures.
  - Only authorized individuals are permitted to move changes into production. Where practical, there is segregation of duties between the staff responsible for moving a change into production and the staff that made the change.

  - An appropriate point of contact for reporting security incidents has been identified and communicated. Some form of incident tracking and escalation is established for significant incidents.
- Backs up, retains, and stores critical financial data and programs. Back-up media is stored in secure locations, both on-site and off-site.
- Reviews general computer controls of critical third party vendors that host and/or support critical financial applications and/or information technology support functions. These controls may be evidenced by an independent third party review and report, such as a SAS 70 Type II report for U.S.-based publicly traded companies.
- Restricts access to facilities to authorized personnel and requires appropriate identification and authentication. Server, telephone, and network and power supply equipment is kept in a secured room or cabinet.

Concerning the company's application software, management:

- Implements data input controls over transactions (including those rejected) to determine that they are authorized, and that transactions accepted are processed correctly and completely. For instance:
  - Procedures are in place to review any data manually entered into the application. These procedures include identifying, correcting, and reprocessing rejected data.
  - Input edits are embedded into the application to check for invalid field lengths, invalid characters, missing or erroneous data, and incorrect dates.
  - Input data is reconciled to source documents through the use of record counts, batching techniques, control totals, or some other type of logging.
  - An authorized person approves input documents. The authorization levels of assigned approvers also are reviewed to determine whether they are reasonable.
- Implements output controls that assess whether input errors are reported and corrections are made or data is resubmitted, preventing the possibility of incomplete or inaccurate data. For instance:
  - Output data is balanced or reconciled to source documents, and there is adequate segregation of duties for the balancing/reconciliation process.
  - Methods for balancing and correcting errors in output are explained.
  - Output is reviewed for general acceptability and completeness, including any control totals.
  - Error reports and/or logs contain information such as a description of problems/errors, date identified, and corrective action taken. These reports and/or logs are reviewed on a timely basis by appropriate personnel.
- Employs a patch management process that includes testing prior to release of packaged software updates into production, or contracts with a third party to test application and system patches. The level of detailed testing depends on the complexity and nature of the change.

- Uses a more formal process for selecting new packages, which includes:
  - Senior management and/or steering committee approval
  - Risk assessment
  - Consideration of application controls
  - Consideration of security requirements
  - Consideration of data conversion requirements, including interfaces
  - Testing
  - Implementation requirements, including back-out plans
  - Post implementation reviews.
- Identifies critical end-user applications, including spreadsheets and other user-developed programs. Critical end-user applications are stored on secured file servers.

Approaches Smaller Companies with Custom Software and with a More Complex Information Technology Environment Can Take to Achieve the Principle

In addition to the approaches described above, a company with custom or in-house software and with a more complex information technology environment applies the following approaches.

Concerning the company's infrastructure, management:

- Develops system development and deployment policies and procedures that address critical financial applications that support relevant assertions related to significant accounts and disclosures in the financial statements. The critical controls include:
  - Establishment of an Information Technology Steering Committee or Change Control Board to review and approve all significant technology initiatives and changes to technology applications and systems.
  - Identification of the magnitude of the risk associated with the changes resulting from a significant systems development or deployment project (high, medium, low)
  - Documentation of all medium and high risk changes on a change request form that includes change requirements, approvals, operational and security impact of the change, back-out plan, and personnel involved in the rollout and testing.
  - Use of version controls to manage access and updates to the code.
  - Segregation of development, test and production environments with access controlled by responsibility.
  - Development and approval of a testing checklist for all medium- and high-risk changes prior to testing.
  - Execution of testing of all medium and high risk changes based on the testing checklist prior to release into production.
  - Obtaining final approvals and sign off by management and end-users.
  - Migration of the change to production only by authorized individuals with proper segregation.
  - Conduct of a post implementation review for all high risk changes.

- Receives reports of both security and processing problems from an appropriate, identified point of contact. Some form of problem tracking is established for significant incidents.
- Puts in place a more formal process to prioritize, report, analyze, and resolve critical problems impacting the company's operations and critical financial data.
- Establishes a help desk and a problem management process, including an escalation procedure for unresolved problems.

Concerning the company's application software, management, in addition to standard input and output controls:

- Uses data processing controls for accuracy, completeness, and timeliness of data during either batch or real-time processing by the computer application. Controls over application programs and related computer operations are reviewed to determine that data is processed accurately through the application and that no data is added, lost, or altered during processing. For instance:
  - The processing of data through the application is documented, for example, by narratives on how the application processes data, flowcharts, or explanations of system or error messages.
  - For applications "run" on a regular schedule, documented procedures explain how this is performed, including related controls.
  - Where a processing log exists, it is reviewed for unusual or unauthorized activity.
  - A processing log, or another log or report, is used to document errors or problems encountered during processing. Information retained includes descriptions of errors encountered, dates identified, any codes associated with errors, any corrective action taken, and date and time of correction.
  - Procedures are in place to control the processing of correct generation/cycle files, including the generation of back-up files from processing to be used for disaster recovery.
  - Processing edits are used. These are similar to input edits but are applied to data during processing.
  - Audit trails are generated during processing. These audit trails are logs or reports that contain information about transactions, including who initiated each transaction, the date and time of the transaction, and the location of the transaction origination (e.g., IP address).

Examples of Effective Ways for Smaller Companies with Packaged Software to Achieve the Principle

Reviewing Logical Security

Management of a software company reviews logical security controls over the financial reporting processes and systems to prevent unauthorized access using the following groupings:

- **Access Controls** – There are formal user account set-up and maintenance procedures to request, establish, issue, suspend, change and delete user accounts. Users are defined as any persons attempting to access a system (e.g. employees, temporary workers, vendors, and contractors).
- **Authentication Controls** – Authentication standards exist that establish the minimum requirements for unique user IDs and passwords, and a finite number of login attempts. Exceptions to the standards are approved by senior management. Unique user IDs afford management the opportunity to log and audit the use of the account and to attribute the use to an individual rather than a group.
- **Privileged Accounts** – Access by system and application administrators (super users) is limited. In a small company there may only be only one employee responsible for information technology security management. Specific attention should be paid to the concentrated powers afforded these employees and controls should be in place to counter potential risks such as segregation of duties issues.
- **Auditing Controls** – A process is in place to periodically review who has access to critical financial data and configuration settings for critical applications and systems. Any violations detected are reported to management.

Using Password Access

A manufacturer of plastic toys set its password standards or critical applications, databases, operating systems, and networks so that passwords:

- Are at least six alphanumeric characters
- Cannot be easily guessed
- Are reset every 90 days
- Are locked out after three consecutive failed login attempts
- Are remembered and cannot be reused for five changes.

Managing Changes to Packaged Software

A manufacturer of plastic toys utilizes the following change management procedures for implementation of a major upgrade to its packaged general ledger software:

- Documents the major change request with a description of the impact of the upgrade, including the impact to the security environment and access controls.
- Documents a back-out plan should the upgrade not perform as expected.
- Develops a plan to test that the edit and validation rules work properly, desired system functions operate properly and produce the desired results, undesired processing results are prevented, and existing technical capabilities continue to work properly.
- Executes, documents, and communicates the results of the tests prior to release into production.
- Maintains a change control log.
- Obtains approval from management and end users of the test results prior to release into production.

Some applications may not support all of the above access controls. In that event management should review what other mitigating access controls exist such as strong network access controls.

Reviewing a Third-Party Vendor

The same manufacturer of plastic toys stores out sources the hosting and support of the critical financial systems to a third party provider. The company:

- Reviews and approves the third party contract and confirms that the third party has signed a non-disclosure agreement.
- Assigns an individual to manage the relationship.
- Reviews annually a third-party SAS 70 Type II report to identify any deficiencies noted regarding the third party's information technology computer controls. All client consideration noted in the report are addressed by management.

Assessing Spreadsheets

To assess how the company uses spreadsheets, management in a professional services organization groups spreadsheets into the following categories:

- **Operational Spreadsheets** – Used to facilitate tracking and monitoring of workflow to support operational processes, such as a listing of open claims, unpaid invoices, and other information that previously would have been retained in manual, paper file folders. These spreadsheets are used to monitor financial transactions and determine that they are captured accurately and completely.

- **Analytical/Management Information Spreadsheets** –Used to support analytical review and management decision making. They are used to evaluate the reasonableness of financial amounts.
- **Financial Spreadsheets –** Used to directly determine financial statement transaction amounts or balances that are populated into the general ledger and/or financial statements.

The company uses a combination of the following controls to help mitigate the risks inherent in its spreadsheet environment:

- **Change Control** – Maintaining a controlled process for requesting changes to a spreadsheet, making changes, and then testing the spreadsheet and obtaining formal sign-off from an independent individual that changes are functioning as intended.
- **Version Control** – Ensuring only current and approved versions of spreadsheets are used, by creating naming conventions and directory structures.
- **Access Control** (e.g., Create, Read, Update, Delete) – Limiting access at the file level to spreadsheets on a central server and assigning appropriate rights. Spreadsheets also are password protected to restrict access.
- **Input Control** – Performing reconciliations evaluating the completeness and accuracy of data input, which is done either manually or systematically through downloads.
- **Security and Integrity of Data** – Implementing a process that secures data embedded in spreadsheets. This is done by "locking" or protecting cells to prevent inadvertent or intentional changes to standing data. In addition, the spreadsheets themselves are stored in protected directories.
- **Documentation** – Ensuring that the appropriate level of spreadsheet documentation is maintained and kept up-to-date as evidence of the business objective and specific functions of the spreadsheet. Development Lifecycle – Applying a standard software development lifecycle to the development process for more critical and complex spreadsheets covering standard phases: requirements specification, design, building, testing, and maintenance.
- **Development Lifecycle** – Applying a standard software development lifecycle to the development process for more critical and complex spreadsheets covering standard phases: requirements specification, design, building, testing, and maintenance.
- **Back-ups** – Implementing a process to back up spreadsheets on a regular basis so that complete and accurate information is available for financial reporting.
- **Archiving** – Maintaining historical files no longer available for update in a segregated drive and locking them as "read only."
- **Logic Inspection** – Inspecting the logic in critical spreadsheets by someone other than their user or developer, and formally documenting the review.

- **Segregation of Duties/Roles and Procedures** – Defining and implementing roles, authorities, responsibilities, and procedures for functions such as ownership, sign-off, segregation of duties, and usage.
- **Overall Analytics** – Implementing analytics as a detective control to find errors in spreadsheets used for calculations. (However, analytics alone are not a sufficient control to completely address the inherent risk of generating financial amounts using spreadsheets.)

Additional Examples of Effective Ways for Smaller Companies with Custom Software and a More Complex Information Technology Environment to Achieve the Principle

Reviewing Logical Security

Using the same example as above for a company with packaged software, the access, authentication and privileged controls would be the same. A company with custom software or a more-complex information technology environment typically would require more robust auditing controls.

Auditing Controls – Critical applications and systems generate security logs and user activity is monitored and logged. Security violations are reported to senior management. Additionally, a process is in place to periodically review access rights to critical financial data and configuration settings for critical applications and systems.

Setting Parameters for Restricting External Connectivity

The information technology group in a smaller pension fund administrator configures, maintains and monitors its firewall to:

- Limit the number of accounts that are provided to firewall administrative personnel.
- Add a "drop all" rule for packets that do not match all the rules and log such information.

The administrator also configures its routers with the following standards:

- The enable password on the router is kept in a secure encrypted form.
- The number of users who can access routers and enable access only through specific network hosts is limited.
- Limit unnecessary e-directed broadcasts, including:
  - Incoming packets at the router sourced with invalid addresses
  - TCP small services
  - UDP small services
  - All source routing
  - All web services running on routers

- Unnecessary ports on routers are disabled.
- The wireless access point's configuration is set where the SSID is not in broadcast mode and passwords are changed from the default.

Managing Change to Custom Software

Management of a manufacturing company has decided to make significant modifications to its inventory management software. The company has only two developers on staff and will need to rely on those individuals to develop, test and migrate the software to production. Additionally, the company does not have an automated code promotion utility to control versions and migrations to the production environment. In this situation the standard controls relevant to segregation of duties may be obtained though:

- Clear identification and risk analysis of the changes that will be required.
- Assignment of the changes to the developers so that each developer works on only those changes assigned to him/her.
- Having the developer who was not responsible for working on the change execute he testing and migration of the change to production.
- Review by management.

Manual controls may be relied on to manage the code version and migration issues and include:

- Creating a manual log of version of the code copied to the development environment with date and time and manually tracking the version of the code migrated to test and then to production.
- Review of all version control procedures prior to moving the code to production by the individual responsible for the information technology functions, who is independent of the change/migration process.

Summary

Control activities are policies and procedures that address risks to the achievement of financial reporting objectives. When selecting control activities, management considers cost relative to potential effectiveness. A particular challenge for smaller businesses is attaining appropriate segregation of duties and resources to manage their information technology systems.

Smaller companies often place greater reliance on monitoring controls and on compensating controls to overcome these challenges. Such reliance also reduces the cost of adding resources to further segregate duties.

6. INFORMATION AND COMMUNICATION

Information and communication represents a company's processes for gathering key financial information to support the achievement of financial reporting objectives. The company needs to identify, capture, process, and distribute financial information to support its control processes. All personnel need to receive clear messages from senior management that internal control over financial reporting is critical to the company and must be taken seriously.

Information systems in smaller organizations are likely to be less formal than in large organizations, but their role is just as significant. Internally generated data can be processed effectively and efficiently in most organizations, regardless of size. Information systems in smaller companies typically identify and report relevant external events, activities, and conditions, but their effectiveness usually is affected substantively by and is dependent on top management's ability to monitor external events.

Effective internal communication between top management and employees may be easier to achieve in a smaller or mid-sized company than in a large one, due to the smaller company's size and its fewer levels, and greater visibility and availability of the CEO. In effect, internal communication takes place through the daily meetings and activities in which the CEO and top management participate. Without the formal communications channels typically found in larger enterprises, many smaller companies achieve effective communication through more frequent day-to-day contacts coupled with an open door policy for senior executives. Top management actions also can also speak louder than words in interactions with company employees, customers, and suppliers.

Information and Communication Principles

The key principles of the information and communication component cover information needs (a managerial focus) and information controls (a technology focus), and the forms of communication – from management, to management, with the board of directors, and with external parties.

COSO has identified six major principles related to the achievement of control objectives at the information and communication level. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section IV of Appendix B

15. ***Information Needs*** – Information is identified, captured and used at all levels of a company to support the achievement of financial reporting objectives.
16. ***Information Control*** – Information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the

company's control processes to support the achievement of financial reporting objectives.

17. ***Management Communication*** – All personnel, particularly those in roles affecting financial reporting, receive a clear message from top management that both internal control over financial reporting and individual control responsibilities must be taken seriously.

18. ***Upstream Communication*** – Company personnel have an effective and nonretributive method to communicate significant information upstream in a company.

19. ***Board Communication*** – Communication exists between management and the board of directors so that both have relevant information to fulfill their roles with respect to governance and to financial reporting objectives.

20. ***Communication with Outside Parties*** – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Information Needs

Basic Principle

Information is identified, captured and used at all levels of a company to support the achievement of financial reporting objectives.

Attributes of the Principle

- *Used to Effect Control* – Information is used in controlling activities, processes, and functions, all of which lead to reliable financial reporting.
- *Operating Information* – Operating information used to develop accounting and financial information often serves as a basis for reliable financial reporting. Operating information also may be the source of many accounting estimates.
- *Internal and External Sources* – Information is developed from internal and external sources. Information is used, among other purposes, for adjusting entries and accounting estimates, as well as to monitor the reasonableness of recorded transactions.

Approaches Smaller Companies Can Take to Achieve the Principle

- In assessing information needs, companies review what information is used to manage day-to-day operations and how this information relates to accounting and to financial reporting.
- Companies obtain information from external sources, such as industry publications, to identify events affecting industry trends, suppliers, customers and competitors, and the general economic climate.
- Management in charge of financial reporting may meet periodically with representatives from other areas of the business – such as operations, compliance, human resources, or product development – to obtain information that may affect financial reporting.

Examples of Effective Ways to Achieve the Principle

Using Management Meetings to Validate and Document Key Assumptions

The CEO of a small manufacturer has all department heads, including the CFO, meet quarterly to validate and document all key assumptions that drive the company's reserves and accruals – including legal, severance, and contracting accruals. Accuracy of these quarterly valuations also is discussed and tracked. These reviews are evidenced by minutes of the meetings.

Using Operating Information for Financial Reporting

A smaller manufacturer with eight plants has an individual responsible for environmental and other regulatory compliance matters who meets regularly with financial management to discuss compliance matters and related remediation costs, to enable appropriate financial reporting of these activities. Such meetings are evidenced through meeting agendas and attendee listings.

Identifying Key Indicators to Improve Performance Monitoring

The CFO of a small consulting firm determined that for his company there were five key performance/control indicators that managers should watch continually, and confirmed that performance on those five indicators – dealing with the management of receivables, expenses, pricing, engagement staffing, and staff productivity – had a high correlation with financial reporting outcomes. The use of these led to improved controls and performance monitoring, and substantive improvements in business performance. Management reports now stress these five indicators. The use of these leading indicators is evidenced by the management reports and the correlation analysis.

Information Control

Basic Principle

Information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives.

Attributes of the Principle

- *Formality* – Information systems can be either formal or informal.
- *Capture Data* – Data underlying financial statements is captured (optimally, at the source) completely, accurately, and timely, in accordance with the company's policies and procedures, and in compliance with laws and regulations.
- *Exception Reporting* – Information control includes exception reporting that triggers prompt exception resolution, root-cause analysis, and control updates.
- *Quality Review* – The quality of system-generated information is reviewed periodically to assess its reliability and timeliness in meeting the company's internal control objectives related to financial reporting.
- *Updated* – Information systems are updated to support the identification and management of risks to reliable financial reporting.

Approaches Smaller Companies Can Take to Achieve the Principle

- Process owners develop and maintain information maps – spreadsheets that display, in the rows, the information elements; and in the columns, the processes and activities performed, by business function that use the information for financial reporting.
- A company uses the risk assessment process to identify risks associated with systems and related changes. The systems or surrounding conditions may change, and the controls (such as access, or back-up) related to the systems are also subject to change. The company uses information maps that describe:
  - Control activities such as batch proofs of system-generated information, confirmation of the consistency of input and output, or similar procedures
  - How system-generated information is reviewed and how these reviews are monitored and tested.
  - Control activities used to monitor and confirm the completeness, accuracy, timeliness, and compliance (with policies and procedures).

Examples of Effective Ways to Achieve the Principle

Updating Information Systems to Support Risk Assessment

The CEO of a small manufacturer continually reviews risks to the company. As part of those reviews, the CEO asks the information technology manager to comment on any changes in systems use, and in personnel or infrastructure; and also asks all other managers to comment about any effects changes in their processes and activities may have on systems. These reviews and the ensuing assessments are evidenced as part of the risk assessment process.

Evaluating the Impact of Information System Changes on Internal Control

A mid-sized automotive parts manufacturer is scheduling a major financial application software upgrade. Using risk-assessment analysis, the company evaluates the impacts of the system changes on the organization's applications and internal controls. Based on this analysis, the company defines the scope of preproduction testing, the need for changes in procedures, and the adequacy of related controls. The documented analysis is evidence of this review.

Using Software to Enable Integration of Process, Control, and System Documentation

The compliance manager (an assigned duty of the CFO, not a full-time role) of a small service provider uses a documentation software tool that enables integrating process, control, and system documentation. The information systems are identified as tools supporting the process in this integrated documentation, and the relevant features are identified as inputs to the process, activity, and control steps. Such integration has reduced the costs of initiating and maintaining control documentation. The compliance manager reviews the documentation with the technical division of the software company and also uses a knowledgeable technology consultant to provide an independent review and opinion. These reviews are evidenced and made available to the CEO.

Using Information Maps in Accounts Payable

A company captures information about its accounts payable process using information maps. Authorizations are used by both role and specific name; and they are shown to be created by the controller, authorized by the CEO, and used by accounting and accounts payable, information technology, materials management, purchasing, and receiving. The information map describes the use of information for control, as well as a basis for monitoring and testing the operation of controls. The company also looks beyond internally generated information and uses these maps to trace information to its sources – for example, vendors' invoices, customers' payment information, and the like – and to confirm information from those sources.

Information Element	Accounting	Accounts Payable	CEO	Controller	Information Technology	Materials Management	Purchasing	Receiving
Accounting								
Account description	C	U	M	M	U	U	U	U
Account code	C	U	M	M	U	U	U	U
Authorization								
Role	U	U	A	C	U	U	U	U
Name	U	U	A	C	U	U	U	U
Purchasing								
Item code	U	U	M	A	C	M	U	U
Item description	A	U	M	U	U	C	U	U
Item quantity	U	U	M	A	U	U	C	U
Item price	U	U	M	A	U	U	C	U
Vendor								
Vendor address	U	U	M	M	U		C	
Vendor code	U	U	M	A	C	U	U	U
Vendor name	U	U	M	A	U	U	C	U
	Roles – (C)reate/modify, (A)pprove, (U)se, (M)onitor							

Developing and Maintaining Information Maps

The treasurer of a small service provider reviews the information maps to determine that they are current and that they show the control activities relating to the quality of system-generated information. If they do not, the treasurer notifies the compliance manager to update the information maps. With updated information maps, the treasurer reviews the batch input–output controls and the flow input–output controls as these activities occur and are monitored by the activity owners.

The treasurer provides evidence that these monitoring activities and reviews have occurred by initialing the documents or by logging the review into a personal journal. The treasurer also confirms that data for key control indicators is recorded and plotted, for completeness, timeliness, accuracy, and compliance, by relevant process, and that the results are within acceptable levels. Periodically, the treasurer reviews the underlying design of the key control indicators, updates it if necessary, and evidences that these control activities have occurred.

The treasurer has correlated the key control indicators (KCIs)[13] to financial statement outcomes, and has found that the KCIs are fairly reliable in projecting financial performance. As a consequence, she has gotten the management team to use the KCIs for purposes of projecting likely changes in performance and as a means of addressing both changes in business plans and disclosure about expected changes in performance. The key control indicator reports are evidence of these monitoring activities.

[13] Described in greater detail in the *Monitoring* chapter

Management Communication

Basic Principle

All personnel, particularly those in roles affecting financial reporting, receive a clear message from top management that both internal control over financial reporting and individual control responsibilities must be taken seriously.

Attributes of the Principle

- *Program Development* – Management develops and implements a communications program that continually reinforces the objectives of internal control.
- *Communications Programs and Approaches* – Management develops a communications program to enable each individual to understand the company's internal control objectives and the relevant aspects of internal control processes, including how the control processes work and individual responsibilities for achieving internal control objectives.

  Management develops communications approaches to enable all employees to understand expected ethical behavior, including relationships with outside parties, as well as individual responsibilities for dealing with inappropriate behavior.
- *Frequency* – Management regularly communicates with employees on the regulatory requirements for achieving effective internal control over financial reporting.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company requires annual reviews of, and signed commitments to, position descriptions that include responsibilities for internal control.
- Information is communicated about the company's internal control objectives, the relevant internal control processes and how these processes work, and individual responsibilities in achieving internal control objectives. Such mechanisms include:
  - Broadcast emails and/or voice mails from management reinforcing the company's commitment to internal control over financial reporting, including updates on both internal and external matters, and about regulatory requirements that may affect the company's ability to achieve its internal control objectives
  - Regular organization-wide conference calls or web casts.
- A company develops and maintains an intranet site, read-accessible to all appropriate personnel, for capturing information regarding the company's internal control processes over financial reporting.
- A company requires all new personnel to read and sign a document that describes the company's expectations related to ethical behavior, including relationships with outside parties, as well as individual responsibilities in dealing with inappropriate behavior. These ethical guidelines are posted in common areas and/or on the

company's website, and employees' signed commitments are made electronically through the website.

- A company reviews and confirms that the content dealing with integrity and ethical values is communicated effectively and clearly, to both internal and external parties.
- A company includes in communications programs a concise summary of laws and regulations affecting internal control over financial reporting.

Examples of Effective Ways to Achieve the Principle

Using Communications Programs to Reinforce Internal Control

The CEO of a small manufacturer has a communications program that includes a newsletter, personal visits to work sites and to employee common areas, and participation in training programs. The CEO uses these situations to reinforce the meaning of internal control over financial reporting, how it relates to laws and regulations, and what is expected of the organization and of all employees. The CEO keeps a file of these visits, and their content is evidenced by the newsletter, an agenda, or a memorandum to file.

Using Orientation Sessions to Communicate Behavioral Expectations

A manufacturer with approximately 430 employees requires all new personnel to attend an orientation session, which is repeated monthly. Each new employee is presented with an employee handbook. Each employee also is required to sign a statement that indicates that the individual has read, understands, and will comply with the company's behavioral expectations. The company includes as evidence this signed statement as part of the employee personnel file.

Using an Intranet Site to Communicate Internal Control Objectives

A services firm with approximately 30 autonomous locations worldwide maintains and updates on its intranet documentation related to internal control objectives. This documentation includes flowcharts that depict an overview of the company's internal control system, which allows each employee to identify how his/her role and efforts impact internal control for the company.

Using a Finance Conference to Discuss and Reinforce Internal Control

A company with approximately $80 million in revenue and with several locations holds a semiannual finance conference that is led by the CFO. All of the individual location controllers attend this conference, which the CFO uses as a forum to provide an update on the business. Other topics discussed during this event include:

- Key objectives for the subsequent six months
- Reinforcement of the company's policies related to ethics and integrity
- Importance of control objectives
- Changes to the internal control structure.

To evidence these conferences, the CFO retains the agendas, including comments and feedback received from attendees.

Upstream Communication

Basic Principle

Company personnel have an effective and nonretributive method to communicate significant information upstream in a company.

Attributes of the Principle

- *Enhance Control* – Upstream communication is used by management to improve performance and enhance internal control.
- *Secondary Channels* – Separate lines of communication are in place and serve as a "fail-safe" mechanism in case normal channels are inoperative or ineffective.
- *Compliance* – A company has an effective "whistleblower" process that meets regulatory requirements and promotes internal control.

Approaches Smaller Companies Can Take to Achieve the Principle

- To enhance employee awareness of a whistleblower hotline, a company includes the hotline number and a brief description of its purpose in the employee handbook, on the company's intranet, and/or on signs posted in high-traffic areas throughout the company's office(s). Additionally, the company augments the hotline to allow for other suggestions dealing with improvements in internal control. This hotline is managed either internally by the company or externally by a third party.
- A company provides an organizational alternative to a line manager – either a coaching or mentoring program, or a professional or technical reporting channel as well as the line reporting channel – so that employees are comfortable that they can be heard.
- A company puts mechanisms in place that allow for a direct line of communication with senior management, such as:
  - A "reply" button at the bottom of the CEO's broadcast email to all employees, which when used generates an email directly to the CEO.
  - An "open door" policy under which members of senior management set aside posted times monthly when they are accessible to any individual throughout the organization.
  - Holding "town hall" meetings periodically at each of the company's locations, at which senior management fields questions, comments, and/or concerns from participants, particularly relating to the company's internal control over financial reporting.
- A company organizes a body of employee representatives that holds periodic meetings with senior management. Prior to these meetings, employee representatives solicit questions, suggestions, and/or concerns from their constituents, with the intent of presenting these to senior management during the meetings.

Examples of Effective Ways to Achieve the Principle

Using a Staff Council to Facilitate Upstream Communication

A $55-million dollar manufacturing company formed a staff council comprising a group of employees who represent the entire workforce, with each employee group having a representative on the council. On a regular basis, members of senior management, including the CEO, meet with this council to discuss "hot topics" affecting the company. Senior management uses these meetings to emphasize its commitment to ethics and integrity, to provide a brief business update, and to solicit feedback on policy changes that are being considered. The employee representatives use these meetings to voice any questions or concerns that have been received from their respective constituents over the period, to provide suggestions to improve processes, and to provide feedback on ongoing employee programs. To evidence the occurrence and content of these meetings, minutes are taken and published in the company's newsletter, which is distributed to all employees monthly.

Establishing a Mentoring Program to Facilitate Upstream Communication

A smaller professional services company established a mentoring program whereby each employee is assigned a coach; they meet periodically or as needed to discuss specific topics, such as the employee's performance and goals. This mentoring program provides an alternative to the employee's line supervisor for discussing and reporting concerns on matters such as compensation, operations, or controls.

Engaging a Third Party to Design and Maintain a Communications Program

The CEO of a small consulting firm had outside counsel design and maintain a process that covers whistleblowing, questions, and suggestions. Users can protect their anonymity, or can choose to name themselves regarding suggestions. The CEO and the board periodically review the process, the status of matters entered into the process, and the results of investigations of those matters. Minutes of these meetings are retained to evidence that these reviews have taken place.

Board Communication

Basic Principle

Communication exists between management and the board of directors so that both have relevant information to fulfill their roles with respect to governance and to financial reporting objectives.

Attributes of the Principle

- *Open Channels* – An open communications channel exists between management and the board of directors.
- *Timely* – The effectiveness of the board of directors is supported by timely communications.
- *Information Needs* – Management considers board needs in developing information requirements.
- *Access to Information* – The board has access to information sources outside of management, on a regular basis and as needed, including access to the external auditors, the internal auditors, and other relevant parties (such as regulatory authorities).

Approaches Smaller Companies Can Take to Achieve the Principle

- At board, and board committee meetings, the CFO reviews financial information and discusses issues that relate to control over financial reporting.
- The board of directors and the internal auditors meet periodically and also whenever events or circumstances warrant. These meetings are used to discuss, in an open environment, the internal auditors' observations about the company's internal control over financial reporting.
- In addition to formal board and board committee meetings, a company has regularly scheduled informal calls between the board and senior management.
- A company establishes and maintains a schedule of formal reporting by management to the board; these reports include updates of financial information as well as related dashboards.
- A company established a formal policy for specific decisions or events that require discussion with or approval from the board, as well as a calendar for the timing of these discussions.

Examples of Effective Ways to Achieve the Principle

Facilitating Communication Between the CEO and Board

The CEO and the chair of the board of a small manufacturing firm talk at least weekly, and more frequently if the need arises. Board members can raise questions, which the chair organizes and presents to the CEO. The CEO often has members of the management team respond directly, copying her on the answer, to get to the root of the issue as well as to give members of the management team more exposure to the board and to the governance processes. The chair keeps a record of these matters, as part of the board minutes.

Using Teleconferences to Communicate with the Board

The CEO, through the corporate secretary, retains emails that arrange teleconferences with the board and that identify who was invited and who attended, and what was discussed. Reports that contain financial results, and related analyses that support internal control over financial reporting, are sent to the board and attached to the emails that evidence the meetings.

Communication with Outside Parties

Basic Principle

Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Attributes of the Principle

- *Open Channels* – Open external communications channels exist to and from customers, consumers, end users, suppliers, and other external stakeholders – shareholders, regulators, financial and other analysts, and affected public groups.
- *Secondary Channels* – A whistleblower process is available to and from outside parties.
- *Value Sharing* – Ethics and values are routinely shared with employees and include expectations about interactions with external parties.
- *Reviewed* – Financial reports are reviewed and evaluated for reliability and transparency by management prior to release.
- *Independent Assessment* – Achievement of internal control over financial reporting is assessed, where required, periodically by external auditors, and this assessment is communicated by management to shareholders and relevant regulatory agencies.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company makes a whistleblower phone number or email account available to outside parties to facilitate the receipt of feedback from customers, suppliers, and other external parties. The number and/or email account is disseminated via the company's website, by marketing materials, and on invoices sent to customers. This is particularly important as a way of receiving feedback from company vendors who may not feel they are treated fairly, or who may receive pressure for "informal" kickbacks.
- A company distributes customer satisfaction surveys from time to time. Included in these surveys are questions related to the customer's perception of ethics and integrity regarding both the entity and the main customer contact. These surveys are controlled by company personnel that are independent of the main customer contacts, to reinforce the integrity of the information.
- A company provides external parties, in addition to their primary contact, either formal or informal contact, as necessary but at least annually, with key members of other departments.
- A company establishes a disclosure committee to coordinate and focus management review of external reporting of financial results.
- A company agrees with outside parties to make available any whistleblowing information that involves them.
- A company makes all employees aware of its policies for dealing with external parties, such as gifts, unusual requests or treatment, and so forth, through:

- Distributed statements of codes of ethics and values
- Periodic training programs
- The intranet.

Examples of Effective Ways to Achieve the Principle

Facilitating Communication with Customers

A manufacturing company with a single location developed a policy whereby at least two members of management, independent of the customer's primary contact, engage in either formal or informal communications with each of the company's customers as necessary, but at least annually. These discussions not only provide a sounding board for the company's customers, but also enable the company to update its understanding of both the customer's business and external factors affecting the customer. This has led to the sharing of information to improve the accuracy and timeliness of sales and receivables information, and also has served to strengthen customer relationships. These discussions are evidenced through documentation by management relating to specifics of each customer conversation, including the customer contact, the date of the conversation, and individual topics discussed, including any action items from either party and their resolution.

Facilitating Communication to and from External Parties

A small retail chain includes on its website a telephone number that can be called with questions, concerns, complaints, and the like. Matters that are reported using this telephone number are recorded and addressed, and this log is presented to the board and attached to the board minutes; and is part of the internal control review. Also, the CFO has discussed with outside parties how they prefer to receive communications from the company's employees. Most external parties noted that they would prefer that communication pertaining to financial reporting come from the CFO. The CFO has in place a process whereby questions and concerns about financial reporting are accumulated through the upstream communications process. The CFO retains the communications as evidence.

Summary

Information and communication address how a company identifies, captures, and distributes information that enables it to prepare reliable financial reporting. Information requirements for external reporting are set for all public companies by regulatory bodies. The extent of information required for reporting depends largely on the complexity of the company's operations.

Small businesses may have a unique advantage communicating financial activity given fewer levels within their structure and greater visibility of the CEO and CFO

7. MONITORING

Monitoring represents a company's processes to determine whether internal control over financial reporting is operating effectively and financial reports are reliably and accurately prepared. Monitoring requires mechanisms for capturing and reporting identified internal control deficiencies. These deficiencies are reported to and addressed by management.

Ongoing monitoring processes enable management to determine whether internal control over financial reporting is present and functioning, often by identifying activities and outcomes that are out of the norm, unexpected, or inconsistent with management's objectives. Managers of smaller businesses have firsthand knowledge of business units. They know, from first hand monitoring of operations, a great deal about the company. By appending monitoring of controls into routine monitoring of operations, management can integrate monitoring of internal control at lesser cost.

Ongoing monitoring activities of smaller companies are more likely to be hands-on and to involve the CEO, CFO and other key managers. Their monitoring of controls is typically a by-product of monitoring the business, accomplished through hands-on involvement in most, if not all, facets of operations. Their close involvement in operations often brings to light significant variances from expectations and inaccuracies in operating or financial data. Management of a smaller business is typically visible, through visits to the factory floor, assembly facility, or the warehouse. Direct knowledge of significant customer and vendor complaints, as well as any communications from regulators, may also alert management about operating or compliance problems that could signal a breakdown which may have financial reporting consequences.

Prior to the release of Section 404 of the Sarbanes-Oxley Act, smaller companies were less likely to undergo separate evaluations of their internal control systems. The need for separate evaluations may be partly offset by highly effective ongoing monitoring activities. Some companies may have an internal auditor who performs separate evaluations. Even smaller companies might assign accounting personnel certain job functions that serve to evaluate controls.

Still another option is to outsource either part or all of the internal audit function, with the outsourcer reporting directly to top management and/or directly to the audit committee. Sometimes accessing outsourced resources, which are a "variable" cost, is considered preferable to committing to additional in-house resources or hiring additional staff, often viewed as a "fixed" cost or as a more permanent cost in the long run.

Due to the more limited organizational structures and the wider spans of control that management often has in smaller companies, deficiencies surfacing from monitoring procedures can be communicated easily to the right person. Personnel in a smaller company usually have a clear understanding of the types of problems that should be

reported upstream. An executive responsible for the payroll function who has an intimate knowledge of labor costs will know immediately if there are cost overruns or whether reported costs are in line with normal operations.

Each organization also should identify and individual responsible for determining the cause of a problem and taking corrective action. The identification of a responsible individual is as important in a smaller organization as it is in a larger one.

Monitoring Principles

COSO has identified three major principles related to the achievement monitoring. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section V of Appendix B.

21. ***Ongoing Monitoring*** – Ongoing monitoring processes enable management to determine whether internal control over financial reporting is present and functioning.

22. ***Separate Evaluations*** – Separate evaluations of all five internal control components enable management to determine the effectiveness of internal control over financial reporting.

23. ***Reporting Deficiencies*** – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

Ongoing Monitoring

Basic Principle

Ongoing monitoring processes enable management to determine whether internal control over financial reporting is present and functioning.

Attributes of the Principle

- *Built-in* – Ongoing monitoring is built into operations throughout a company. This monitoring includes explicit identification of what constitutes a deviation from expected control performance and thereby signals a need to investigate both potential control problems and changes in risk profiles.
- *Feedback* – Ongoing monitoring provides continual feedback on the effective operation of controls integrated into processes, and on the processes themselves.
- *Indicator of Control Effectiveness* – Ongoing monitoring can serve as a primary indicator of internal control operating effectiveness and new or changing risks to company objectives.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company includes supervisory activities, consisting of recording metrics about control – completeness, timeliness, accuracy, and compliance – in processes so that current performance can be tracked and compared with target performance.
- A company provides monitoring control charts to reviewers – usually the supervisors of those with first-level accountability for processes and activities and their controls – for use in confirming that control performance is on track, that deviations are being investigated and resolved, that the right metrics are being monitored, and that there is integrity to the monitoring process.
- A company confirms that operations metrics that are monitored have a reasonable correlation to financial reports and hence can be used as an indicator of changes impacting financial reporting.

Examples of Effective Ways to Achieve the Principle

Using Built-in Operating Measures and Key Control Indicators

A CFO uses operating measures and key control indicators (KCIs) for all major accounting and financial processes that have been determined to present material risk to the reliability of the financial statements. These processes include "manage accounts receivable," "manage payroll," "manage accounts payable," and "prepare and present financial statements." In accounts payable, for example, KCIs focus on the accuracy, timeliness, completeness, and compliance of documents received for vouching, and then in turn on the accuracy and timeliness of checks prepared. Targets consistent with risk assessments have been set and performance is tracked to target. Results are shared with the management team and also are used for performance appraisals and related development programs. The CFO has assigned reviews to different people. The CFO reviews the accounts payable KCIs and confirms that performance is at target or better and that issues are being investigated and resolved. To evidence these reviews, the KCI listings and evidence of the reviews are retained by management.

Ongoing Monitoring as an Indicator of Control Effectiveness

The production team for a dairy processor with five autonomous plants performs some aspect of inventory cycle counting on a daily basis. The production team has developed a systematic process by which the higher volume items are counted more frequently; however, the full inventory balance is counted at least annually. All counts are performed "blind;" that is, the count teams do not have access to the inventory balance in the company's perpetual inventory system. When the cycle count is completed, the count teams compare their counts results to amounts in the company's perpetual inventory system. All variances are investigated, and efficiency is tracked; the corporate cost accountant reviews cycle counting efficiency daily to confirm that the error rate is within an acceptable range and that any variances are handled appropriately. To evidence this review, the cost accountant signs off on the daily cycle counting sheets, which include documentation on resolution for all variances.

Using Operating Information to Aid in Monitoring

The sales team for a cooperative uses its central finance function to maintain a sales target report. This report contains daily sales information and highlights sales that are guaranteed or on consignment. Weekly, the controller reconciles actual sales from this report to the company's general ledger system, with all discrepancies researched and resolved. The vice president reviews the reconciliation and evidences his review by signing.

Firsthand Knowledge of the Rhythm of a Business

A local manufacturer with several operating facilities has approximately 100 employees between union labor, supervisors, managers, and executives. There are two shifts and all plants operate with one production line six days a week. Each location has approximately the same number of employees, and the accounting is centralized at headquarters. The CFO has been with the company for over ten years and thoroughly understands each business process. Weekly payroll summary reports are reviewed by the CFO, who is also heavily involved with developing the company's budget. Based on his years and background with the company, the CFO understands the seasons, cycles, and workflow of the operation. The flat organizational design and smaller size of this company allows the CFO to immediately determine the cause – a particular project, expected overtime, hiring, layoffs, and so forth – and take corrective action, if necessary. The combination of this depth of knowledge and span of control is a sound basis for effective monitoring. The evidence of the monitoring maybe accomplished by documenting the review or by the corrective action taken.

Separate Evaluations

Basic Principle

Separate evaluations of all five internal control components enable management to determine the effectiveness of internal control over financial reporting.

Attributes of the Principle

- *Objective* – Separate evaluations provide an objective look at the overall internal control over financial reporting as of a point in time. Separate evaluations of internal control for external reporting are performed by someone who can provide an objective review and who is not involved in the activities being reviewed.
- *Knowledgeable* – The evaluator understands the components being evaluated and how they relate to the activities supporting the reliability of financial reporting.
- *Feedback* – Separate evaluations are used to provide feedback on the effectiveness of ongoing monitoring procedures.
- *Scope and Frequency* – Management varies the scope and frequency of separate evaluations depending on the significance of risks being controlled and importance of the controls in mitigating those risks.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company uses an internal audit activity to provide an objective perspective on the overall effectiveness of the internal control structure, including ongoing monitoring. Internal audit reports are distributed to senior management and the audit committee.
- A company uses qualified internal resources or outside parties to conduct separate evaluations.
- A company develops a self-assessment questionnaire for a business process to serve as a diagnostic reference point focusing on the extent to which those responding to the survey believe that controls related to the business process are being applied.
- A penetration review of the computer network is performed periodically, with identified security issues concerning access to financial data addressed and resolved in a timely manner.

Examples of Effective Ways to Achieve the Principle

Using an Independent Party to Perform Separate Evaluations

The CFO of a small manufacturer has contracted with an independent party to test the effectiveness of ongoing monitoring of the internal control components. The results from the tests, as well as the underlying monitoring results, are considered in determining the frequency and scope of future testing cycles. These findings are recorded and become part of the internal control and testing processes.

Determining the Scope and Frequency of Separate Evaluations

Periodically, the CEO of a small injection molding company requires its internal audit function to perform separate evaluations of business processes for the purpose of providing feedback on the effectiveness of ongoing monitoring procedures. The scope and frequency, which are agreed to by the internal audit director, senior management, and members of the board, depend primarily on the significance of the risks being controlled and the importance of the controls in reducing risks to an acceptable level. Prior to commencement of these reviews, the internal audit director determines that the staff (internal audit or otherwise) assembled to perform the reviews can be objective about the process controls to be reviewed, have a general understanding of both the process and the overall internal control structure, and understand the objectives of the review. Subsequent to the review, the internal audit director distributes a report on the process controls reviewed to appropriate members of senior management and the board. The content of this report includes:

- The scope of the work performed, including identification of the process and controls evaluated
- Descriptions of the actual operation of the ongoing monitoring controls over the process, as compared with the design of the controls
- Documentation of any identified deficiencies and management's response and proposed remediation

To evidence this evaluation, members of senior management sign the report thereby evidencing their individual reviews and the appropriateness of remediation of any identified deficiencies.

Reporting Deficiencies

Basic Principle

Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

Attributes of the Principle

- *Timely Action* – Reports from both internal and external sources are considered for their internal control implications, and timely corrective actions are identified and taken.
- *Findings Reported* – Findings of an internal control deficiency – including systems and data security control weaknesses—are reported to the individual who owns the process and control involved and who is in position to take corrective actions. The findings also are reported to at least one level of management above the process owner.
- *Deficiencies Reported* – Deficiencies that affect internal control over financial reporting are communicated to top management and the board or audit committee, regularly and as necessary.

Approaches Smaller Companies Can Take to Achieve the Principle

- A company reports deficiencies to the board, which helps its members, and especially the members of the audit committee, perform their oversight function. The items are reported individually or in a summary report, depending on their nature.
- A company establishes procedures and assigns responsibility to individuals to monitor reports from external parties, including external auditors and regulators. The individuals review the reports and carefully consider internal control implications.
- A company establishes an alternative channel for reporting deficiencies that are considered sensitive in nature, such as illegal or improper acts. Such reports are directed to a member of senior management or the board, depending on the nature of the action and the individuals involved.
- A company establishes a protocol in which all financial reporting deficiencies, regardless of materiality, are reported to an individual and at least one level of management above that person, both of whom are in positions and have the authority to take corrective action. The nature and materiality of the financial reporting deficiency dictate the level of the individuals to whom the deficiency is reported.

Examples of Effective Ways to Achieve the Principle

Reporting Observed Control Deficiencies to Management

At a small travel agency with one location, employees are organized into several teams based on functional responsibilities, and each team has a leader who is typically a member of management. The teams meet weekly for approximately 30 minutes to discuss, among other things, ways to improve the internal control structure and address control deficiencies. Depending on the nature and materiality of matters raised by the team, the leaders deal with the reported deficiencies as appropriate. A member of the team prepares minutes of each meeting and distributes them to the entire team via email.

Reporting Observed Control Deficiencies and Resolution to the Board

The board of a small company has taken a direct role in receiving a log of deficiencies and their resolution. The accountable party is notified of the deficiency, with the relevant supervisor informed, and corrective action is requested and logged.

Reporting Observed Deficiencies to the Board

A company developed a report of significant deficiencies and material weakness, and a summary report of minor deficiencies, which are presented to the board and appended to the board minutes, and are used as part of the review of internal controls.

Summary

Monitoring represents a company's ongoing processes to assess the design and operating effectiveness of all five internal control components. Monitoring requires processes to capture and report identified control deficiencies so that they can be addressed by management on an ongoing basis.

Ongoing monitoring activities of smaller companies are more likely to be hands-on and to involve the CEO, CFO, and other key managers. Often their monitoring is a by-product of monitoring the business through management's firsthand knowledge of business operations. The close interaction by management often brings control deficiencies to light.

Smaller businesses often place greater reliance on monitoring activities as part of their overall internal control structure. Cost and effort can be reduced to the extent that monitoring is built into processes.

8. ROLES AND RESPONSIBILITIES

Internal control over financial reporting is affected by a number of parties. The board of directors (directly or through its audit committee), management, internal auditors, and other personnel all make important contributions through their roles and responsibilities. There is a distinction between those who are directly part of a company's internal control activities – such as management and those accountable for internal control over financial reporting – and those who are indirectly involved, but the actions of all parties nonetheless can assist in the achievement of effective internal control over financial reporting.

The purpose of this chapter is not to repeat the principles, attributes, and examples of the five components of internal control, which are found in the preceding five chapters; but to put them in the context of the roles that various parties play with regard to internal control over financial reporting and to identify how these roles translate into specific responsibilities.

Roles and Responsibilities Principles

COSO has identified three major principles related to the achievement of control objectives at the roles and responsibilities level. Those principles are summarized below and detailed in the balance of this chapter. Additional guidance that may be used for assessing the presence and functioning of these principles and attributes is included in Section VI of Appendix B.

24. ***Management Roles*** – Management exercises responsibility and ownership for internal control over financial reporting.

25. ***Board and Audit Committees*** – The board of directors, directly and through the audit committee, has processes that provide directors with information needed to perform their oversight responsibilities regarding the achievement of effective internal control over financial reporting.

26. ***Other Personnel*** – All company staff accept responsibility for actions that directly or indirectly impacts financial reporting.

Management Roles

Basic Principle

Management exercises responsibility and ownership for internal control over financial reporting.

Attributes of the Principle

- *Top Management Responsibility* – The CEO and senior management are responsible for sound internal control over financial reporting, including both initiating and maintaining the program.

  Senior and functional management are responsible for ensuring all employees understand the importance of complying with internal control objectives through adherence to internal control policies and procedures.
- *Finance and Accounting Officers Monitor and Provide Oversight* – Finance and accounting officers monitor and provide oversight of the accounting, finance, and reporting functions of an organization.

Approaches Smaller Companies Can Take to Achieve the Principle

- Position descriptions and both business and management objectives are used to reinforce management's responsibility for strong internal control over financial reporting.
- The CEO and senior management provide oversight of internal control over financial reporting by:
  - Displaying accountability and responsibility for establishing and maintaining internal control over financial reporting
  - Confirming that all position descriptions address responsibilities for internal control over financial reporting
  - Supervising organizational units and taking responsibility for internal control over financial reporting related to unit objectives
  - Insisting that plans are developed for initiating internal control programs, and that the plans are followed.
- Finance and accounting officers provide oversight of internal control over the financial reporting process through:
  - Reviewing and approving documentation for significant transactions
  - Actively participating in departmental meetings
- Mid-level management reinforce responsibilities for internal control over financial reporting by:
  - Identifying deficiencies and inefficiencies in internal control over financial reporting within their functional areas and taking corrective action
  - Reviewing and approving activities and controls

  - Monitoring the control activities of those who report to them.
- Management reacts to legislative and regulatory changes that may impact internal control over financial reporting.
- Management evaluates information obtained through incidental interactions – with customers, vendors, distributors, banks, or other external parties – that might have implications for the company's internal control over financial reporting.

Examples of Effective Ways to Achieve the Principle

CEO and Board Input to Developing Roles

Due to significant changes occurring within the company and the industry, the CEO established an initiative to work directly with the board of directors to refine, and in some cases to develop, roles for each level of the company's management team. Once established, an off-site meeting was held where goals and objectives of the business, along with specific responsibilities, were outlined and communicated directly to senior and mid-level management. Everyone heard a consistent message and understood how they would interact with one another and could participate in providing adequate controls within the organization. Evidence that this mechanism is in place is provided by the company's policies and procedures established to define and communicate key roles and responsibilities for management surrounding, in particular, internal control over financial reporting. These policies and procedures are easily accessible on the company's intranet.

Top Management Acknowledgment of Roles

In another company, senior management reinforces the responsibilities for internal control over financial reporting throughout the organization by requesting mid-level managers to sign subcertifications based on their roles. This request provides internal accountability for company-wide assertions. Evidence that this mechanism is in place is the quarterly certifications regarding compliance with internal control over financial reporting submitted to senior management by each operating manager or department leader.

Reviewing and Updating Roles and Responsibilities

A newly hired controller of a company, while reviewing the roles and responsibilities of the employees in her department, noted that the accounts payable manager had the ability to edit the vendor master file and to issue checks to these same vendors. These responsibilities represent a clear "segregation of duties" deficiency. Members of management had great faith in the ethical conduct of the accounts payable manager, who was a well-respected senior employee. To mitigate the risk without inhibiting efficient workflow, the controller requested that the information technology department generate a weekly report of all edits to the vendor master file so she could review it for unusual changes. The review of the weekly edit reports, and the sign-off by the controller, provide evidence that this mechanism is in place. Further, the company's documented roles and responsibilities outline each employee's day-to-day responsibilities.

Board and Audit Committee

Basic Principle

The board of directors perform their oversight responsibilities relating to the achievement of effective internal control over financial reporting.

Attributes of the Principle

- *Governance, Guidance, and Oversight* – The board of directors provides governance, guidance, and oversight related to internal control over financial reporting. Management is accountable to the board of directors.
- *Balance* – The board of directors balances its role of advising management with its fiduciary duty to monitor and oversee management.
- *Audit Committee* – The board often relies on an audit committee to assist with its oversight responsibilities. The audit committee of the board is responsible for hiring the external auditors. The audit committee also holds executive sessions with both internal and external auditors to obtain feedback on their audits and the identification of control deficiencies.

Approaches Smaller Companies Can Take to Achieve the Principle

- The board of directors through the corporate bylaws, and the audit committee through its charter, set forth their roles and responsibilities.
- The audit committee is responsible for reviewing significant findings of the internal audit activity and periodically meets with the internal audit director in private, executive sessions.
- The audit committee meets periodically with the internal and external auditors.

Examples of Effective Ways to Achieve the Principle

Board Governance, Guidance, and Oversight

The responsibilities of the company's board of directors are defined in the corporate bylaws, and the audit committee's responsibilities are defined in its charter. A component of the audit committee's charter requires an annual review to confirm that it reflects current activities of the committee and is consistent with the committees mandate and objectives. The board of directors and audit committee annually review and approve their bylaws and charter, respectively, and record evidence of their reviews.

Audit Committee Governance, Guidance, and Oversight

Quarterly, a company's board of directors requires the audit committee to report directly to the board on matters related to the financial reporting process; internal control, including any deficiencies identified; and the information technology environment. Further, the audit committee meets with the board of directors quarterly and they evaluate jointly any financial reporting issues. Evidence that this mechanism is in place is contained in the board of directors' by-laws, which require such reporting; in a pre-meeting package for the meetings; and in the minutes documenting the meetings.

Other Personnel

Basic Principle

All company staff accept responsibility for actions that directly or indirectly impacts financial reporting.

Attributes of the Principle

- *Everyone has responsibility* – Roles and responsibilities related to financial reporting are well defined and communicated to help implement effective internal control over financial reporting.
- *Upstream communication* – Staff communicate to higher company levels problems involving financial reporting, noncompliance with the code of conduct, and other deviations from company policy or illegal acts.
- *Senior-Level Accountability* – The internal audit activity is accountable to the board of directors and management.
- *Objective Assessment* – The internal audit activity provides objective assessments about the design and the operating effectiveness of components of the organization's internal control over financial reporting.

Approaches Smaller Companies Can Take to Achieve the Principle

- The company's annual personal goal-setting process conducted through the human resource function includes financial reporting objectives for those directly or indirectly involved in the financial reporting process.
- The internal audit activity has a mission statement or charter in place describing its role in monitoring internal control over financial reporting. In addition, the audit committee or board of directors reviews and approves annually the scope of internal audit work.
- The authority of the internal audit activity includes direct and unrestricted access to the audit committee. Regular meetings are scheduled, including sessions where company management is not present.
- The internal audit activity consists of a group of financially literate cross-functional employees or an outsourced function, working under the direction of the audit committee.
- Internal audit work is performed in accordance with the *International Standards for the Professional Practice of Internal Auditing* established by The Institute of Internal Auditors.

Examples of Effective Ways to Achieve the Principle

Reviewing and Approving Internal Audit Plan

Annually, a company's internal audit director presents for review and approval to the audit committee internal audit's charter and its defined roles and responsibilities. In addition, the internal audit director reviews the internal audit group's scope and work plan for the current year with management and the audit committee. Evidence that this mechanism is in place is the approved charter and current-year scope and work plan document.

Cross-Business-Unit Reviews

A company utilizes the services of two competent financial employees from business unit A to periodically monitor internal control over financial reporting of business unit B. The employees report their findings and recommendations throughout the year to management and the audit committee. Evidence that this mechanism is place is the employees' findings and recommendations.

.

Cosourcing Internal Audit

The Chief Audit Executive (CAE) at a smaller retail outlet supplements internal audit needs with qualified third party audit providers to obtain needed skills and experiences in specific audit areas. The .CEO oversees the work of the auditor, reviews all internal audit reports drafted and reports to the Audit Committee on the outcome of all projects.

Outsourcing Internal Audit

A small manufacturing company outsources its internal audit activity to a third party that specializes in such services. In order to monitor and control this outsourced function, the engagement leader of the internal audit outsourcer meets quarterly with the CEO and audit committee chair to discuss the work that the internal audit outsourcer has performed and its findings, the work that the internal audit outsourcer plans to perform, and any risks or concerns the engagement leader may have. Evidence that this mechanism is in place is the quarterly written report provided by the internal audit outsourcer to the company, which contains work to date, recommendations with management responses, and future audit plans.

Operations Manual as Basis for Evaluation

A company has a number of operating locations that are relatively similar in nature and structure. An operating manual is provided to each location, covering instructions on both operational and financial tasks. The company instructs its internal audit group to test internal controls in these areas to determine whether the locations are in compliance with the operations manual. Evidence that this mechanism is in place is the internal audit group findings reported to the audit committee on a timely basis.

A. EVALUATION MATRIX AND ILLUSTRATIVE TEMPLATES – OVERVIEW

The appendices to this guidance include a series of illustrative tools and templates that may assist management in evaluating the effectiveness of internal control over financial reporting. The evaluation matrix and templates are illustrative and represent possible tools, but not the only tools, that may be used in determining whether the organization has effectively implemented all principles included in this guidance. Nor are the individual tools intended to represent a complete set of all criteria that a company will consider in its evaluation of internal control over financial reporting.

For each of these templates, users are reminded that these are illustrations only and companies should review to determine what additional questions are required for its business.

Appendix B – Evaluation Matrix

This matrix summarizes the twenty-six principles and related attributes described in this guidance. While attributes associated with each principle and are generally expected to be present, it is possible to accomplish a principle without addressing each individual attribute, depending on unique factors in each company. Management is encouraged to consider the combination of entity-level controls and process level controls when evaluating the presence and functioning of principles and attributes. In addition, there may be minor trade-offs between certain principles within a component. Accordingly, management is encouraged to summarize at the end of each component how processes set forth accomplish the specified component principles.

Appendix C – Illustrative Entity-wide Controls Evaluation Matrix

This appendix illustrates how a company may review its entity level controls. In this example, the company has used the Evaluation Matrix presented in Appendix B, and completed its documentation of control and evidence of control. This questionnaire does not contain questions related to control activities as the controls relied on by management are at the process level.

Appendix D - Illustrative Account Estimates, Adjusting Entry and Closing Evaluation Entry Matrix

This appendix illustrates how a company may review process level controls related to account estimates, adjusting entries, and closing process. In this example, the company has expanded the control evaluation matrix presented in Appendix B to include more detailed financial reporting assertions (control objectives), risks, and control activities present. This control matrix provides management with a basis to conclude on principles 11 - 14 in the Evaluation Matrix.

Appendix E – Sample Process Level Risk and Control Matrix

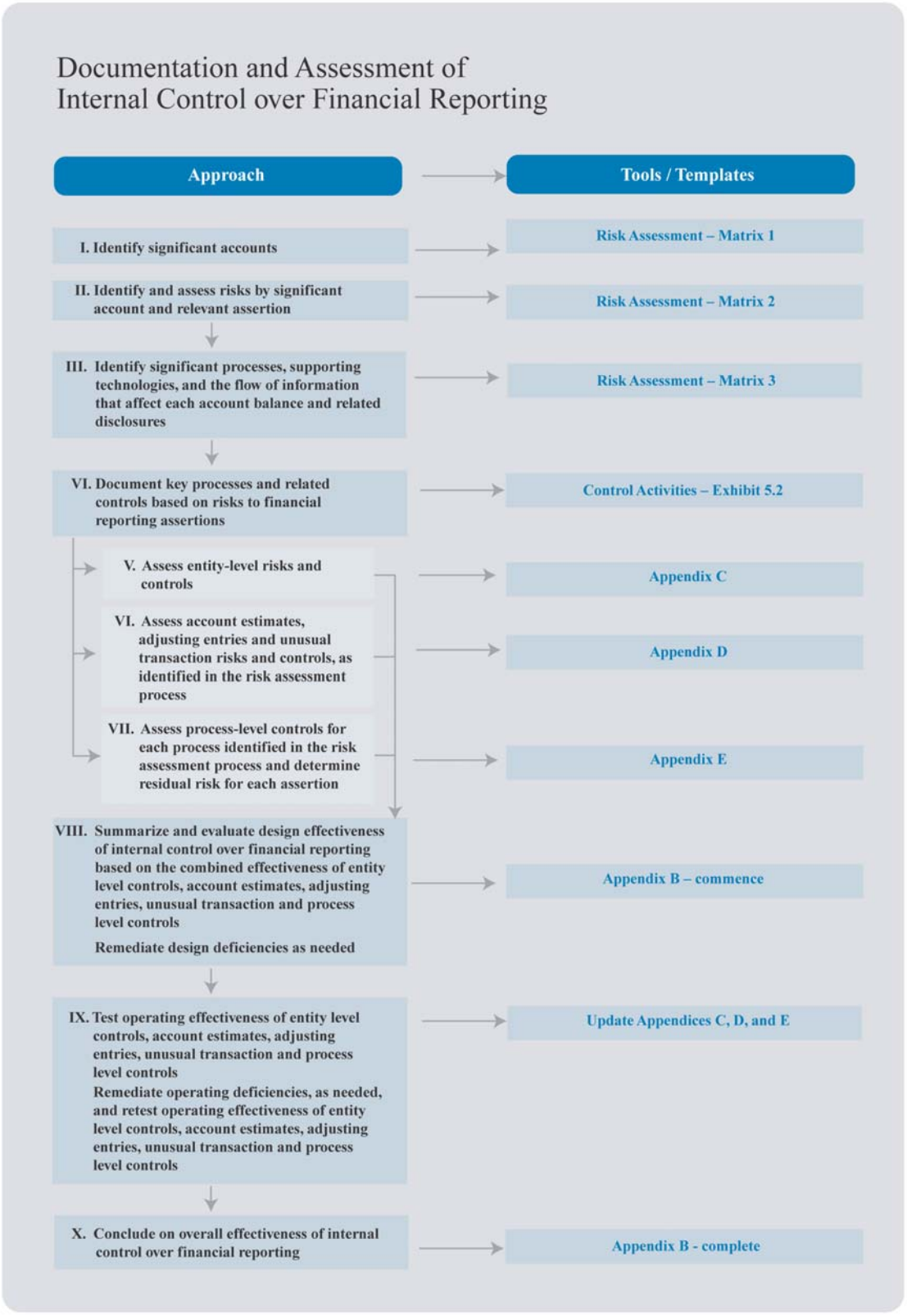
This appendix illustrates how a company may review process level controls related to a specific process, being the revenue cycle. In this example, the company has expanded the control evaluation matrix presented in Appendix B to include more detailed financial reporting assertions (control objectives), risks, control activities, plus a summary of whether the control is either manual or automated and whether the control is preventive or detective.

This control matrix provides management with a basis to conclude on principles 11 - 14 in the Evaluation Matrix. However, to fully consider these principles, management will need to review each question in Appendix E in relation to the specific processes identified in the risk assessment process. Common processes, as noted in the risk assessment chapter, for evaluation may include:

- Capital assets
- Equity
- Financial statement close and reporting
- Financing
- Payroll and employee benefits
- Purchase and payables
- Revenue and receivables
- Taxes
- Treasury

Using These Templates

A company may choose to use only one, several or an entire set of templates similar to those presented. When used together, the templates provide management with the basis for concluding on the overall effectiveness of internal control over financial reporting. A process diagram noted on the following page details the flow between these templates and other examples and exhibits presented in this guidance.


Documentation and Assessment of
Internal Control over Financial Reporting
Approach
Tools / Templates
I. Identify significant accounts
Risk Assessment – Matrix 1
II. Identify and assess risks by significant account and relevant assertion
Risk Assessment – Matrix 2
III. Identify significant processes, supporting technologies, and the flow of information that affect each account balance and related disclosures
Risk Assessment – Matrix 3
VI. Document key processes and related controls based on risks to financial reporting assertions
Control Activities – Exhibit 5.2
V. Assess entity-level risks and controls
Appendix C
VI. Assess account estimates, adjusting entries and unusual transaction risks and controls, as identified in the risk assessment process
Appendix D
VII. Assess process-level controls for each process identified in the risk assessment process and determine residual risk for each assertion
Appendix E
VIII. Summarize and evaluate design effectiveness of internal control over financial reporting based on the combined effectiveness of entity level controls, account estimates, adjusting entries, unusual transaction and process level controls
Remediate design deficiencies as needed
Appendix B – commence
IX. Test operating effectiveness of entity level controls, account estimates, adjusting entries, unusual transaction and process level controls
Remediate operating deficiencies, as needed, and retest operating effectiveness of entity level controls, account estimates, adjusting entries, unusual transaction and process level controls
Update Appendices C, D, and E
X. Conclude on overall effectiveness of internal control over financial reporting
Appendix B - complete

The templates illustrated also are shown at various stages of completion, as would normally occur using the above approach, as follows:

- The *Evaluation Matrix* is blank, before the other templates have been completed and summarized.
- The *Illustrative Entity-Wide Controls Evaluation Matrix* is presented following the completion of Step IV above. In this example, management has completed its evaluation of the design of internal control. They have provided evidence of the control but have not yet competed the evaluation of operating effectiveness.
- The *Illustrative Account Estimates, Adjusting Entry and Closing Evaluation Entry Matrix* is presented in progress as it may occur during the completion of Step V above. In this example management has completed its assessment of the design of the internal controls as being high, medium or low but has not yet undertaken its evaluation of operating effectiveness.
- The *Illustrative Process Level Risk and Control Matrix* is also presented in progress, as it may occur during the completion of Step VI above. In this example, management has not yet concluded its evaluation of design effectiveness.

B. EVALUATION MATRIX

I.	Control Environment Principles [14]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
1	**Integrity and Ethical Values** - Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for financial reporting.					
1.1	Has top management *developed* a clearly articulated statement of values or ethical concepts that are understood by key executives and the board?			Yes/No		Yes/No
1.2	Has top management *communicated* its commitment to ethical values and reliable financial reporting through words and actions?			Yes/No		Yes/No
1.3	Has the importance of integrity and ethical values been communicated and *reinforced* to all employees in a manner that is consistent with the organizational culture?			Yes/No		Yes/No
1.4	Are processes in place to *monitor* the company's compliance with principles of sound integrity and ethical values?			Yes/No		Yes/No
1.5	Are *deviations* from sound integrity and ethical values identified in a timely manner and addressed and remedied by appropriate levels of the organizations?			Yes/No		Yes/No

[14] *Italicized* text in principle boxes refer to the stated attributes in Chapter 3 – Control Environment

I.	Control Environment Principles [14]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
2	**Importance of Board of Directors** - The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.					
2.1	Is the board of directors actively involved in *evaluating and monitoring risk* of management override of internal control?			Yes/No		Yes/No
2.2	Does the board monitor and evaluate the risks affecting the reliability of financial reporting?			Yes/No		Yes/No
2.3	Does the board of directors, through the audit committee, provide effective board-level *oversight* of the effectiveness of internal control over financial reporting and the preparation of financial statements for external purposes?			Yes/No		Yes/No
2.4	Does the audit committee provide effective board-level *oversight* of the work of the external auditors			Yes/No		Yes/No
2.5	Does the audit committee have the exclusive authority to hire, fire, and determine the compensation of the external audit firm?			Yes/No		Yes/No
2.6	Does the board of directors have a majority of members who are independent?			Yes/No		Yes/No
2.7	Does the board of directors have a *critical mass* of members who are independent of management?			Yes/No		Yes/No
2.8	Does the audit committee have a majority of members who are *independent*?			Yes/No		Yes/No
2.9	Does the board of directors and audit committee have one or more members who have *financial expertise*			Yes/No		Yes/No

I.	Control Environment Principles [14]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
2.10	Does the board of directors and audit committee meet *frequently* enough to address important oversight responsibilities?			Yes/No		Yes/No
2.11	Does the board of directors and audit committee meet a sufficient amount of time in executive sessions?			Yes/No		Yes/No
3	**Management's Philosophy and Operating Style** - Management's philosophy and operating style support achieving effective internal control over financial reporting.					
3.1	Does management's philosophy and operating style *set the tone* that high-quality and transparent financial reporting are expected?			Yes/No		Yes/No
3.2	Does management establish and clearly *articulate financial reporting objectives*, including goals related to internal control over financial reporting?			Yes/No		Yes/No
3.3	Does management follow a disciplined, objective process in selecting accounting *principles* and developing accounting *estimates*?			Yes/No		Yes/No
4	**Organizational Structure** - The company's organizational structure supports effective internal control over financial reporting.					
4.1	Does management *establish internal reporting responsibilities* for each functional area and business unit in the organization that are consistent with the objective of achieving effective internal control over financial reporting?			Yes/No		Yes/No
4.2	Does management *maintain an organizational structure* that facilitates			Yes/No		Yes/No

I.	Control Environment Principles [14]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
	effective reporting and other communications about internal control over financial reporting among various functions and positions of management?					
4.3	Do management's lines of reporting recognize the importance of *maintaining processes* for objective verification of information reported to the public?			Yes/No		Yes/No
5	**Commitment to Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.					
5.1	Are *competencies* that support accurate and reliable financial reporting *identified*?			Yes/No		Yes/No
5.2	Does the company *retain* or otherwise utilize *individuals* who possess the required competencies related to financial reporting?			Yes/No		Yes/No
5.3	Are needed *competencies* regularly *evaluated* and maintained?			Yes/No		Yes/No
6	**Authority and Responsibility** - Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.					
6.1	Does the board of directors provide effective *oversight* management's process for defining responsibilities for key financial reporting roles?			Yes/No		Yes/No
6.2	Are the assignment of *responsibility* and delegation of authority clearly defined for all employees involved in the financial reporting process?			Yes/No		Yes/No
6.3	Does the assignment of authority and responsibility include appropriate			Yes/No		Yes/No

I. Control Environment Principles [14]		Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
	limitations, such as proper segregation of duties to minimize the risk of financial misstatements?					
7	**Human Resources** - Human resource polices and practices are designed and implemented to facilitate effective internal control over financial reporting.					
7.1	Does management *establish human resource policies* and procedures that demonstrate its commitment to integrity, ethical behavior, and competence?			Yes/No		Yes/No
7.2	Are employee *recruitment and retention* for key financial positions guided by the principles of integrity and by the necessary competencies associated with the positions?			Yes/No		Yes/No
7.3	Does management support employees by providing access to the tools and *training* needed to perform their financial reporting roles?			Yes/No		Yes/No
7.4	Do employee *performance* evaluations and the company's *compensation* practices support the achievement of financial reporting objectives?			Yes/No		Yes/No
In summary, are the processes set forth sufficient to accomplish the seven control environment principles identified and support the achievement of the company's objectives related to financial reporting?						
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.						

II.	Risk Assessment Principles [15]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
8	**Importance of Financial Reporting Objectives** - A precondition to risk assessment is the establishment of objectives for reliable financial reporting.					
8.1	Do financial reporting objectives align with the requirements of *generally accepted accounting principles?*			Yes/No		Yes/No
8.2	For each significant account and disclosure, are financial reporting objectives linked to *financial statement assertions* that underlie a company's financial statements, noting those assertions that are more important/ relevant depending on the circumstances?			Yes/No		Yes/No
8.3	With respect to financial statement accounts and disclosures, is significance based on *materiality* and risk, considering both quantitative and qualitative factors, according to SEC Staff Accounting Bulletin 99?			Yes/No		Yes/No
9	**Identification and Analysis of Financial Reporting Risks** – The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.					
9.1	Are *risks potentially* impacting the achievement of financial reporting objectives identified?			Yes/No		Yes/No
9.2	Does the company's risk identification include *business processes* that potentially impact financial statement accounts and			Yes/No		Yes/No

[15] *Italicized* text in principle boxes refer to the stated attributes in Chapter 4 – Risk Assessment

II. Risk Assessment Principles [15]		Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
	disclosures?					
9.3	Are *information technology* infrastructure and processes supporting the financial reporting objectives included in the financial reporting risk assessment?			Yes/No		Yes/No
9.4	Does risk identification consider both *internal and external factors* and their impact on the achievement of financial reporting objectives?			Yes/No		Yes/No
9.5	Has the organization put into place effective risk assessment mechanisms that *involve appropriate levels of management?*			Yes/No		Yes/No
9.6	Are identified risks analyzed through a process that includes estimating the potential *impact* of the risk and an assessment of the *likelihood* of the risk occurring?			Yes/No		Yes/No
9.7	Has management established *triggers for reassessment* of risks as changes occur that may impact financial reporting objectives?			Yes/No		Yes/No
10	**Assessment of Fraud Risk** - The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.					
10.1	Are fraud assessments an *integral part* of the risk identification and analysis process?			Yes/No		Yes/No
10.2	Does the company's' assessment of fraud risk consider *incentives and pressures*, attitudes, and rationalizations, as well as opportunity to commit fraud?			Yes/No		Yes/No
10.3	Does the company consider risk factors relevant to its industry and to the geographic region where it does business?			Yes/No		Yes/No

II. Risk Assessment Principles [15]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
10.4 Does the company consider the potential for fraud in *high-risk areas*, including – revenue recognition – management override – accounting estimates – significant unusual accounts – nonstandard journal entries – significant intercompany accounts, and – vulnerabilities related to misappropriation of assets?			Yes/No		Yes/No
10.5 Does the audit committee understand and exercise oversight of management's fraud risk assessment processes?			Yes/No		Yes/No
10.6 Does the board of directors actively evaluate and monitor risk factors affecting the reliability of financial reporting, including the risk of management override?			Yes/No		Yes/No
In summary, are the processes set forth sufficient to accomplish the three risk assessment principles identified and support the achievement of the company's objectives related to financial reporting?					
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.					

III. Control Activity Principles [16]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
To fully consider principles 11 through 14, management will need to review each question in relation to the specific processes identified in the risk assessment process. Common processes, as noted in the risk assessment chapter, for evaluation may include: – Accounting estimates – Adjustments – Capital assets – Equity – Financial statement close and reporting – Financing – Payroll and employee benefits – Purchase and payables – Revenue and receivables – Taxes – Treasury – Unusual transactions Appendix C contains a sample questionnaire related to account estimates and adjusting entries that, when completed, would form the basis for management to summarize in this matrix key conclusions for each of the following questions. Appendix D contains a sample questionnaire related to one process noted above, being revenue and receivables that, when completed, would form the basis for management to summarize in this matrix key conclusions for each of the following questions. These process level controls also will form the primary reliance for management.					

[16] *Italicized* text in principle boxes refer to the stated attributes in Chapter 5 – Control Activities

III.	Control Activity Principles [16]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
11	**Elements of a Control Activity** - Policies and procedures are established and communicated throughout the company, at all levels and across all functions, that enable management directives to be carried out.					
11.1	Are *policies* in place establishing what should be done, specifying what is allowable or should be done to mitigate risks, including the parameters of acceptable performance?			Yes/No		Yes/No
11.2	Are *procedures* in place to accomplish the policy specifying how the action prescribed is performed, including the parameters of acceptable performance?			Yes/No		Yes/No
11.3	Do control activities reflecting board-level policies *cascade* from the board into the company's functions, departments, and processes?			Yes/No		Yes/No
11.4	Does management establish the criteria for determining the parameters that define "*accomplishment*" of the policy objectives, that is, the criteria relate to the level of processing that sufficiently mitigates risks?			Yes/No		Yes/No
11.5	Are policies and procedures of the company *monitored* and immediate corrective actions taken for exceptions that are not within established tolerances?			Yes/No		Yes/No
11.6	Are procedures designed such that management can *track implementation* and effectiveness of actions taken to manage risks relevant to financial reporting objectives?			Yes/No		Yes/No
11.7	Are policies and procedures that are critical to the accomplishment of financial reporting objectives, as determined from the risk			Yes/No		Yes/No

III. Control Activity Principles [16]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
assessment process, *documented*, and is that documentation is made available to staff as necessary?					
11.8 Does *ownership* of policies and procedures reside with the management of the business or function in which the relevant control risk resides?			Yes/No		Yes/No
12 Control Activities Linked to Risk Assessment - Actions are taken to address risks to the achievement of financial reporting objectives.					
12.1 Do control activities include controls *related to all aspects of the recording process*, including adjusting and closing journal entries and accounting estimates?			Yes/No		Yes/No
12.2 Are control activities over financial reporting *built into* the company's regular business processes and clearly understood by employees?			Yes/No		Yes/No
12.3 Are control activities sufficiently robust to *mitigate risks* impacting financial reporting objectives?			Yes/No		Yes/No
12.4 Is the selection of controls based on the *risk assessment* process, emphasizing processes and also classes of transactions, and financial statement accounts and disclosures that could contain misstatements that individually, or in the aggregate, could have a material impact on the company's financial statements?			Yes/No		Yes/No
12.5 Does the selection of control activities encompass relevant *information technology* controls?			Yes/No		Yes/No

III. Control Activity Principles [16]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
12.6 Are policies and procedures reviewed periodically by management to determine their *continued relevance*?			Yes/No		Yes/No
13 Selection and Development of Control Activities - Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives**.**					
13.1 Do control activities include a *range of activities* that balance cost and effectiveness, depending on the circumstances?			Yes/No		Yes/No
13.2 Does management use an appropriate blend of *preventive* and *detective* controls to mitigate risks to the achievement of financial reporting objectives?			Yes/No		Yes/No
13.3 Does management use an appropriate blend of manual and automated controls, to mitigate risks to the achievement of financial reporting objectives?					
13.4 Within the constraints of available resources, are duties logically *segregated* among people or processes to mitigate risks and meet financial reporting objectives?			Yes/No		Yes/No
13.5 Do *compensating controls* used to counterbalance the effect of limited segregation of duties reduce the residual risk to an acceptable level?			Yes/No		Yes/No

III. Control Activity Principles [16]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
14 Information Technology - Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.					
14.1 Are *application controls* built into computer programs and supporting manual procedures, and designed to provide completeness and accuracy of information processing critical to the integrity of the financial reporting process, authorization, and validity?			Yes/No		Yes/No
14.2 Are *general computer controls* broad and do they include access controls, change and incident management, systems development and deployment, data backup and recovery, third party vendor management, and physical security controls critical to the integrity of the financial reporting process?			Yes/No		Yes/No
14.3 Are *end-user* computing processes, including spreadsheets and other user-developed programs documented, secured, backed-up, and regularly reviewed for processing integrity?			Yes/No		Yes/No
In summary, are control procedures implemented over major transaction cycles, accounting estimates, and the closing process sufficient to support the achievement of the company's objectives related to effective financial reporting? Consider summary conclusions in the context of each of the processes identified above.					
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.					

IV.	Information and Communication Principles [17]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
15	**Information Needs** – Information is identified, captured and used at all levels of a company to support the achievement of financial reporting objectives.					
15.1	Is information used in *controlling activities*, processes, and functions, all of which lead to reliable financial reporting?			Yes/No		Yes/No
15.2	Does *operating information* used to develop accounting and financial information serve as a basis for reliable financial reporting, and is operating information also used as the source of accounting estimates?			Yes/No		Yes/No
15.3	Is there evidence that the company uses relevant information, including data – from business processes – about the state of the economy – economic data affecting the industry and the company's competitive position in the industry – other relevant data in developing its accounting estimates and adjusting entries?			Yes/No		Yes/No
16	**Information Control** - Information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives.					
16.1	Are the procedures sufficiently *formal* such that – management can determine whether the			Yes/No		Yes/No

[17] *Italicized* text in principle boxes refer to the stated attributes in Chapter 6 – Information and Communication

IV.	Information and Communication Principles [17]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	**Process Level**			
	control objectives is being met – documentation supporting this understanding is in place – personnel routinely know the procedures that need to be performed?					
16.2	Are data underlying financial statements *captured* (optimally, at the source) completely, accurately, and timely, in accordance with the company's policies and procedures, and in compliance with laws and regulations?			Yes/No		Yes/No
16.3	Does information control include *exception reporting* that triggers prompt exception resolution, root-cause analysis, and control updates?			Yes/No		Yes/No
16.4	Is the quality of system-generated information *reviewed* periodically to assess its reliability and timeliness in meeting the company's internal control objectives related to financial reporting?			Yes/No		Yes/No
16.5	Are information systems *updated* to support the identification and management of risk to reliable financial reporting?			Yes/No		Yes/No
17	**Management Communication** - All personnel, particularly those in roles affecting financial reporting, receive a clear message from top management that both internal control over financial reporting and individual control responsibilities must be taken seriously.					
17.1	Has management *developed* and implemented a communications program that continually reinforces the objectives of internal control?			Yes/No		Yes/No

IV. Information and Communication Principles [17]		Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
17.2	Has management developed a *communications program* to enable each individual to understand the company's internal control objectives and the relevant aspects of internal control processes, including how the control processes work and individual responsibilities in achieving internal control objectives?			Yes/No		Yes/No
17.3	Has management developed communications *approaches* that specify individual responsibilities in dealing with inappropriate behavior?			Yes/No		Yes/No
17.4	Does management communicate *frequently* with employees on the regulatory requirements for achieving effective internal control over financial reporting?			Yes/No		Yes/No
18	**Upstream Communication** - Company personnel have an effective and nonretributive method to communicate significant information upstream in a company.					
18.1	Is upstream communication used by management to improve performance and *enhance internal contro*l?			Yes/No		Yes/No
18.2	Are *separate lines of communicatio*n in place and do they serve as a "fail-safe" mechanism in case normal channels are inoperative or ineffective?			Yes/No		Yes/No
18.3	Does the company have an effective "whistleblower" process that meets regulatory *compliance* requirements and promotes internal control?			Yes/No		Yes/No

IV.	Information and Communication Principles [17]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
19	**Board Communication** - Communication must exist between management and the board of directors so that both have relevant information to fulfill their roles with respect to governance and to financial reporting objectives.					
19.1	Does an *open communications channel* exist between management and the board of directors?			Yes/No		Yes/No
19.2	Is the effectiveness of the board of directors supported by *timely* communications?			Yes/No		Yes/No
19.3	Does management consider board *information needs* in developing reporting?			Yes/No		Yes/No
19.4	Does the board have *access to information* sources outside of management, on a regular basis and as needed, including access to the external auditors, the internal auditors, and other relevant parties (such as regulatory authorities)?			Yes/No		Yes/No
20	**Communication with Outside Parties** - Matters affecting the achievement of financial reporting are communicated with outside parties.					
20.1	Do *open external communications channels* exist to and from customers, consumers, end users and suppliers, and other external stakeholders – shareholders, regulators, financial and other analysts, and affected public groups?			Yes/No		Yes/No
20.2	Is a *secondary* "whistleblower" process available to and from outside parties?			Yes/No		Yes/No
20.3	Are ethics and *values routinely shared w*ith employees and do they include expectations			Yes/No		Yes/No

IV. Information and Communication Principles [17]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
about interactions with external parties?					
20.4 Are financial reports reviewed and evaluated for *reliability* and transparency by management prior to release?			Yes/No		Yes/No
20.5 Is achievement of internal control over financial reporting *independently assessed*, where required periodically by external auditors, and is this assessment communicated by management to shareholders and relevant regulatory agencies?			Yes/No		Yes/No
In summary, are the processes set forth sufficient to accomplish the six information and communication principles identified and support the achievement of the company's objectives related to financial reporting?					
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.					

V.	Monitoring Principles [18]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
21	**Ongoing Monitoring** - Ongoing monitoring processes enable management to determine whether internal control over financial reporting is present and functioning.					
21.1	Is ongoing monitoring *built into* operations throughout the company, and does it include explicit identification of what constitutes a deviation from expected control performance and thereby signal a need to investigate both potential control problems and changes in risk profiles?			Yes/No		Yes/No
21.2	Does ongoing monitoring provide *feedback* on the effective operation of controls integrated into processes, and on the processes themselves?			Yes/No		Yes/No
21.3	Does ongoing monitoring serve as a primary indicator of both *control operating effectiveness* and of risk conditions?			Yes/No		Yes/No
22	**Separate Evaluations** - Separate evaluations of all five internal control components enable management to determine the effectiveness of internal control over financial reporting.					
22.1	Do separate evaluations provide an *objective* look at the overall internal control over financial reporting as of a point in time, and are separate evaluations of internal control for external reporting performed by someone who can provide an objective review and who is not involved in the activities being reviewed?			Yes/No		Yes/No

[18] *Italicized* text in principle boxes refer to the stated attributes in Chapter 7 – Monitoring

V. Monitoring Principles [18]		Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
22.2	Is the evaluator *knowledgeable* and understand the components being evaluated and how they relate to the activities supporting the reliability of financial reporting?			Yes/No		Yes/No
22.3	Are separate evaluations used to provide *feedback* on the effectiveness of ongoing monitoring procedures?			Yes/No		Yes/No
22.4	Does management vary the *scope and frequency* of separate evaluations depending on the significance of risks being controlled and importance of the controls in mitigating those risks?			Yes/No		Yes/No
23	**Reporting Deficiencies** - Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.					
23.1	Are reports from external sources considered for their internal control implications, and *timely corrective actions* are identified and taken?			Yes/No		Yes/No
23.2	Are findings of an internal control deficiency – including systems and data security control weaknesses—*reported* to the individual who owns the process and control involved and who is in position to take corrective actions, and are the findings also reported to at least one level of management above the process owner?			Yes/No		Yes/No
23.3	Are *deficiencies* that affect internal control over financial reporting communicated to top management and the board or audit committee, regularly and as necessary?			Yes/No		Yes/No

V. Monitoring Principles [18]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	Process Level			
In summary, are the processes set forth sufficient to accomplish the three monitoring principles identified and support the achievement of the company's objectives related to financial reporting?					
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.					

VI.	Roles and Responsibilities Principles [19]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
		Entity level	Process Level			
24	**Management Roles** - Management exercises responsibility and ownership for internal control over financial reporting.					
24.1	Are the CEO and senior management *(top management) responsible* for sound internal control over financial reporting, including both initiating and maintaining the effective internal controls?			Yes/No		Yes/No
24.2	Do *finance and accounting officers monitor and provide oversight* of the accounting, finance, and reporting functions of an organization?			Yes/No		Yes/No
25	**Board and Audit Committees** - The board of directors perform their oversight responsibilities relating to the achievement of effective internal control over financial reporting.					
25.1	Does the board of directors provide *governance, guidance, and oversight* related to internal control over financial reporting, and is management accountable to the board of directors?			Yes/No		Yes/No
25.2	Does the board of directors balance its role of advising management with its fiduciary duty to monitor and *oversee* management?			Yes/No		Yes/No
25.3	Is the *audit committee* of the board responsible for hiring the external auditors and holding executive sessions with them to obtain feedback on the audit and the auditors' identification of control			Yes/No		Yes/No

[19] *Italicized* text in principle boxes refer to the stated attributes in Chapter 8 – Roles and Responsibilities

VI. Roles and Responsibilities Principles [19]	Summary of Controls		Design Effective-ness	Summary Evidence of Control	Operating Effective-ness
	Entity level	**Process Level**			
deficiencies?					
26 Other Personnel - All company staff accept responsibility for actions that directly or indirectly impacts financial reporting.					
26.1 Is internal control over financial reporting the *responsibility of everyon*e in a company that directly or indirectly impacts financial reporting?			Yes/No		Yes/No
26.2 Is that *responsibility* an explicit or implicit part of those individual's job description?			Yes/No		Yes/No
26.3 Is the *internal audit* activity accountable to the board of directors and management?			Yes/No		Yes/No
26.4 Does the internal audit activity provide *objective assessments* about the design and the operating effectiveness of components of the organization's internal control over financial reporting?			Yes/No		Yes/No
In summary, are the processes set forth sufficient to accomplish the three roles and responsibilities principles identified and support the achievement of the company's objectives related to financial reporting?					
Summarize the reasoning for this judgment along with any areas that the company will be addressing to improve the quality of controls over financial reporting.					
In summary, are the processes set forth sufficient to accomplish the all principles from each of the five components that support the achievement of the company's objectives related to financial reporting?					

C. ILLUSTRATIVE ENTITY-WIDE CONTROLS EVALUATION MATRIX

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
Control Environment				
1. **Integrity and Ethical Values** - Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for financial reporting.				
1.1. How has top management *developed* a clearly articulated statement of values or ethical concepts that are understood by key executives and the board?				
1.1.1. Does a code of conduct and other policies exist and does this code include guidance on acceptable business practice, conflicts of interest, or expected standards of ethical and moral behavior, and are effectively implemented within the organization?	Code of conduct is posted on the external and internal website. All company employees receive a copy of code of conduct via email. Code of conduct is also included as part of human resources Handbook as of March 21, 2005.	Y	Reviewed the code of conduct policy and human resource handbook.	
1.1.2. Is there an established "tone at the top" that reinforces acceptable moral guidance about what is right and wrong? How is this tone communicated and practiced by executives and management throughout the organization?	Quarterly all-hands meetings with company top management are held. All Sales Executives must sign a "no side letter agreement" quarterly. Employee handbook contains employee responsibilities in section 19.0	Y	Reviewed the following list a. Side letter collection list from Robert Jones. b. Employee handbook section 19.0 c. CFO's email on Jan 27, 2005	
1.1.3. How does the company attain confidence that dealings with employees, suppliers, customers, investors, creditors, insurers, competitors, and auditors, etc., are ethical (i.e., management conducts business on a high ethical plane, and insists that others do so)?	See #1.1.1 & 1.1.2.	Y		

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
1.2. Has top management *communicated* its commitment to ethical values and reliable financial reporting through words and actions?				
1.2.1. How is management informed of the Company's risk tolerance policies, including the proper approval channels upon executing transactions involving risk?	Executive approval matrices are implemented for all key transactions, including. These amounts are codified in job descriptions and code of conduct.	Y	Reviewed the expense authorization matrix.	
1.2.2. Is there frequent interaction between senior management and operating management.	Sr. management visits the subsidiaries on an ad hoc rotational basis. The CEO meets with the Executive staff at least once a quarter.	Y	Reviewed on-line calendars of CFO and CFO for evidence of recurring meetings.	
1.3. Has the importance of integrity and ethical values been communicated and *reinforced* to all employees in a manner suitable for the organization?	See below 1.3.1.			
1.3.1. Does management acknowledge the importance of the data processing and accounting functions, and show concerns about the reliability of financial reporting and safeguarding of assets.	SOX compliance is a priority, addressing reliability of data and safeguarding. Disclosure committee; sr. manager reads 10-Q and updates for any financial reporting issues on a quarterly basis.	Y	Reviewed SOX project plan.	
1.4. Are processes in place to *monitor* the company's compliance with principles of sound integrity and ethical values?				
1.4.1. Is there a process of periodically assessing compliance with code of conduct is in place?	Code of conduct is sent to all Company employees either via email or new hire orientation.	Y	Reviewed the list with human resources director.	
1.4.2. How does the company attain confidence that strong ethical attitudes and actions toward financial reporting, including appropriate resolution of disputes over application of accounting treatments are maintained (e.g., selection of conservative	Disclosure committee, sales representation letters. Eight audit committee meetings and four board meetings annually.	Y	Reviewed copy of audit committee meeting and board schedule from the CEO's executive assistant. .	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
versus liberal accounting policies; whether accounting principles have been misapplied, important financial information not disclosed, or records manipulated or falsified)?				
1.5. Are *deviations* from sound integrity and ethical values identified in a timely manner and addressed and remedied by appropriate levels of the organizations?				
1.5.1. Are appropriate remedial action taken in response to departures from approved policies and procedures or violations of the code of conduct, and if so what are these actions?	Departures that surface from policies or violations of behavioral expectations are dealt with immediately. Whistleblower Program is in place for employees to report violations.	Y	Reviewed whistleblower site to obtain evidence that comments provided by staff accessing the site are dealt with in accordance with company policy.	
1.5.2. What processes are in place addressing policies detailing remedial action steps are communicated to and understood by all associates?	After the employee training orientation, the employees sign a form expressing they understand that they understand the entire handbook.	Y	Reviewed the form in human resource handbook	
1.5.3. Does management avoid intervening or overriding established controls?	Management has supported the Code of Conduct, and has not attempted to override or bypass controls.	Y	No incident has been reported.	
2. **Importance of Board of Directors** - The board of directors understands and exercises oversight responsibilities related to financial reporting and related internal control.				
2.1. Is the board of directors actively involved in *evaluating and monitoring risk* of management override of internal control?				
2.1.1. Does a process exist for informing the board of significant issues? Is information communicated on a timely basis?	Accounting issues, if any, are discussed by the CFO with chairman of audit-committee, Mr Smith. He may decide	Y	Reviewed audit committee minutes.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
	to engage counsel to investigate if need arises.			
2.1.2. Does the board of directors and/or audit committee give adequate consideration to understanding how management identifies, monitors, and controls business risks affecting the organization?	a. Any strategic and operational risks are discussed with the board. b. Any financial and disclosure risks are discussed with the audit committee during meetings.	Y	Board minutes 9/21/04 Audit committee meeting agenda 3/9/05	
2.2. Does the board of directors, through the audit committee, *oversee* the effectiveness of internal control over financial reporting and the preparation of financial statements for external purposes?				
2.2.1. Does the audit committee represent an informed and vigilant overseer of the financial reporting process and internal controls, including the information systems processing and related controls?	The audit committee receives quarterly reports from management and the internal auditors on the quality of the organization's controls and accounting policies.	Y	Reviewed agenda for audit committee meetings.	
2.2.2. Does the audit committee have a charter outlining its duties and responsibilities? Does the audit committee have adequate resources and authority to discharge its responsibilities?	An audit committee charter is in place.	Y	Reviewed the audit committee charter.	
2.3. Does the audit committee *oversee* the work of the external auditors and have the exclusive authority to hire, fire, and determine the compensation of the external audit firm?				
2.3.1. Does the audit committee meet privately with the external auditors to discuss the reasonableness of the financial reporting process, system of internal control, significant comments, recommendations, and management's performance?	A private session between the audit committee and the external auditors takes place quarterly.	Y	Reviewed meeting minutes.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
2.3.2. Does the audit committee review the scope of activities of the external auditors?	Annual audit plan review. Audit procedures are presented by quarters.	Y	Reviewed the audit committee presentation from Q3	
2.4. Does the board of directors have a *critical mass* of members who are independent of management?				
2.4.1. Does the company have a process to periodically evaluate the independence of outside board, including their affiliations, relationships, and transactions with the company?	The independence of board members is considered as part of proxy process. Proxy questionnaire reviewed by CFO and chief counselor. Nominating committee for the board also exists.	Y	Reviewed to company Proxy.	
2.5. Does the audit committee have exclusive authority to hire, fire, and determine the compensation of the external audit firm?	The audit is tendered each three years, at which time management assessed audit proposals and presents the recommended audit firm to the audit committee	N	None, as the control is not effective. Weakness needs to be considered in context of overall principle.	
2.6. Does the board of directors have a majority of members who are *independent*?	The independence of the board members is considered as part of proxy process. Proxy questionnaire reviewed by CFO and chief counselor. Nominating committee for the board also exists.	Y	Reviewed to company Proxy.	
2.7. Does the board of directors have a critical mass of members who are independent of management?	Mr. Smith, an ex-CFO of XYZ Corp, is the Chair of the audit committee.	Y	Reviewed to Mr. Smith's resume.	
2.8. Does the audit committee have a majority of members who are independent?	Yes, there are no board members on the audit committee that are not independent.			
2.9. Does the company have a process to periodically evaluate the independence of audit committee members, including their affiliations, relationships, and transactions with the company?	The independence of audit committee members is considered as part of proxy process. Proxy questionnaire reviewed by CFO and chief counselor. Nominating committee for the board also exists.	Y	Reviewed to company Proxy.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
2.9.1. Does the company have a process to periodically evaluate the independence of audit committee members, including their affiliations, relationships, and transactions with the company?	The independence of audit committee members is considered as part of proxy process. Proxy questionnaire reviewed by CFO and chief counselor. Nominating committee for the board also exists.	Y	Reviewed to company Proxy.	
2.10. Does the board of directors and audit committee have one or more members who have financial expertise	Mr. Smith, an ex-CFO of XYZ Corp, is the Chair of the audit committee and a CPA	Y	Reviewed to Mr. Smith's resume.	
2.11. Does the board of directors and audit committee meet frequently enough to address important oversight responsibilities?	Yes, meetings are help quarterly	Y	Reviewed Audit Committee minutes for evidence of meeting frequency	
2.12. Does the board of directors and audit committee meet a sufficient amount of time in executive sessions?	Yes, the last agenda item on each meeting is an executive session	Y	Reviewed Audit Committee minutes for evidence of executive sessions	
3. **Management's Philosophy and Operating Style** - Management's philosophy and operating style support achieving effective internal control over financial reporting.				
3.1. Management has not included in its evaluation an assessment of management's philosophy and operating style. Management expects to include this review in the next update of it entity-level controls		N		
4. **Organizational Structure** - The company's organizational structure supports effective internal control over financial reporting.				
4.1. Does management *establish internal reporting responsibilities* for each functional area and business unit in the organization?				
4.1.1. How are modifications to the organizational structure made timely on a timely basis in light of changed conditions?	When an organizational change is made, changes are made in the financial system, which updates the portal.	Y	Printout of an email from Jay, and printout of a portal on his information.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
4.2. Does management *maintain an organizational structure* that facilitates effective reporting and other communications about internal control over financial reporting among various functions and positions of management?				
4.2.1. Are there an appropriate number of people, particularly with respect to data processing and accounting functions, with the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems?	The Accounting Manager, Controller, VP of Finance, and SEC Reporting Manager have prior Big-4 training experiences.	Y	Reviewed resumes.	
4.2.2. Are mechanisms in place for reporting identified internal control deficiencies? How are gaps reported to management?	A process is in place to document internal controls, and exceptions from testing of controls are communicated to Company management accordingly.	Y	Refer to the 404 documentation and testing.	
4.3. Do management's lines of reporting recognize the importance of *maintaining processes* for objective verification of information reported to the public?	Pending review	N		
5. **Commitment to Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.				
5.2. Does the company retain or otherwise utilize individuals who possess the required competencies related to financial reporting				
5.2.1. Is personnel turnover in key functions kept at a minimum, e.g., accounting, and data processing.	Personnel turnover has been at satisfactory levels for the finance dept., with low turnover rates.	Y	Only two employees resigned in Accounting in the past 4 years.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
6. **Authority and Responsibility** - Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.				
6.2. Management has not included in its evaluation an assessment of the authority and responsibility. Management expects to include this review in the next update of it entity-level controls		N		
7. **Human Resources** - Human resource polices and practices are designed and implemented to facilitate effective internal control over financial reporting.	The responsibilities are clearly defined.	Y		
7.1. Does management *establish human resource policies* and procedures that demonstrate its commitment to integrity, ethical behavior, and competence?	A human resources New-Hire checklist is in place for hiring. Training - Training is encouraged and is approved by department head. Promotion - in employee handbook p8 Compensation – Compensation committee is involved only in the executive level. For regular employees, market data is verified before an offer is extended.			
7.1.1. Are key managers' responsibilities clearly defined, and is their understanding of these responsibilities considered adequate?	Detailed roles and responsibilities are defined and communicated annually as part of the overall performance evaluation process	Y	Reviewed job overviews for new hires.	Y
7.1.2. Are policies and procedures for hiring, training, promoting, and compensating employees in place?	The executives have the required experiences to perform their duties.		Reviewed the new-hire check list	Y
7.2. Are employee *recruitment and retention* for key financial positions guided by the principles of integrity and by the necessary	Compensation committee meets about twice a year.	Y		

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
competencies associated with the positions?				
7.2.1. Do executives have the required knowledge, experience, and training to perform their duties?	Background checks have been conducted since May 2004.		Reviewed the published job experiences and personal profiles on intranet website.	Y
7.2.2. Is there appropriate oversight of compensation, retention, and termination of key executives by the board?	Done through Human Resources / Compensation committee of the board		Reviewed the compensation committee minutes.	Y
7.2.3. Are employee candidate background checks performed, particularly with regard to prior actions or activities considered to be unacceptable by the entity?	All information technology staff with responsibilities related to financial reporting attend external training sessions on basic control requirements and have information technology related designations.		Reviewed the background check requirement.	
7.3. Does management support employees by providing access to the tools and *training* needed to perform their financial reporting roles?		Y		
7.3.1. Are information technology personnel adequately trained in their internal control roles and responsibilities?	Job responsibilities such as goals are established quarterly.	Y		
7.4. Do employee *performance* evaluations and the company's *compensation* practices support the achievement of financial reporting objectives?		Y		
7.4.1. Are all staff made aware of their job responsibilities and performance expectations?	Detailed roles and responsibilities are defined and communicated annually as part of the overall performance evaluation process. Performance against corporate goals is communicated quarterly.		Reviewed a copy of quarterly goals.	

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
8. **Risk Assessment**				
8.1. **Importance of Financial Reporting Objectives** - A precondition to risk assessment is the establishment of objectives for reliable financial reporting.	Annual budget is established and updated on a quarterly basis. Periodic forecast update includes capital budget and information technology requirements.			
8.1.1. Do financial reporting objectives align with the requirements of *generally accepted accounting principles?*	Board of directors approves budget.			
8.1.2. Has management established entity-wide objectives, and are those objectives periodically reviewed and updated?	As part of planning process, management prioritizes the initiatives for the upcoming year and the budget is built based on the initiatives.	Y	Reviewed FY 2005 approved budget.	
8.1.3. How are Entity-wide objectives communicated to board of directors?	Risks of doing business are identified and discussed during the executive staff meeting. Executive staff meets periodically and addresses changes (if any).	Y	Reviewed board meeting minutes.	
8.1.4. How are business plans and budgets aligned with entity-wide objectives, strategic plans, and current conditions?		Y	Reviewed FY 2005 approved budget.	
8.1.5. Is a process place for identifying entity-level objectives and changes are modified?			Reviewed the E Staff's meeting schedule.	
Information and Communication				
16. **Information Control** - Information relevant to financial reporting is identified, captured, processed, and distributed within the parameters established by the company's control processes to support the achievement of financial reporting objectives.	There is an information technology org chart in place that supports business needs. Information technology reports to Carolyn.			
16.2. Are data underlying financial statements *captured* (optimally, at the source) completely, accurately, and timely, in accordance with the company's policies and	Yes, information technology initiatives are considered in the broader strategic planning and budgeting process undertaken by management.			

Principle and Attribute	Entity Level Control	Design Effective-ness	Evidence of Control	Operating Effective-ness
procedures, and in compliance with laws and regulations?				
16.2.1. Are information technology plans and structure able to meet the organization's needs?	Yes, initial policies are developing in within the information technology department and subjected to review and revision by the senior information technology staff member. Senior management reviews all significant policies developed by the group.		Reviewed information technology org chart.	
16.2.2. Are information technology initiatives align with the overall objectives of the company?	Management has not included in its evaluation and expects to include this review in the next update of it entity-level controls	N		
16.2.3. Are critical information technology developed and approved by appropriate levels of management?	Management has not included in its evaluation and expects to include this review in the next update of it entity-level controls	N		
16.3. Have service level agreements been, documented, approved, and monitored between the information technology group, outside vendors and the user community?	The company currently has only one contract requiring a SLA, and the key performance measures in the contract are reviewed monthly. The board is apprised annually of overall performance and significant deviations in performance.	Y		

D. ILLUSTRATIVE ACCOUNT ESTIMATES, ADJUSTING ENTRY AND CLOSING ENTRY EVALUATION MATRIX

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
General Ledger Maintenance					
Existence and Completeness – Changes to the Chart of Accounts are processed completely and accurately	Personnel do not appropriately process changes to the chart of accounts. This action may lead to inappropriately mapped financial statements. Personnel do not completely process changes to the chart of accounts. This error may lead to incomplete financial statements.	The Chart of Accounts and related account groupings are reviewed annually for consistency and comparability between the current and previous accounting periods by the Corporate Controller and Accounting Manager.	Manual	Detective	Low
Existence and Valuation – Routine transactions are accurately processed (manually or automatically) in the appropriate accounting period.	Automatic journal entries are not processed accurately in the proper accounting period. These errors may lead to incomplete or inaccurate financial statements. Manual journal entries are not processed accurately in the proper accounting period. These errors may lead to incomplete or inaccurate financial information	Manual journal entries with appropriate back-up are provided to the Senior Accountant for review and are entered into the journal entry log, which is a manually maintained document, and initialed upon approval by the Corporate Controller.	Manual	Preventive	Low
Existence and Completeness –Period-end closing adjustments are recorded completely and accurately.	When preparing period ending closing adjustments personnel do not record all of the appropriate transactions into the general ledger. This may result in incomplete financial statements.	The Senior Accountant maintains a listing of recurring journal entries monthly, including adjusting, reversing, consolidating, and eliminating journal entries, to	Manual	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
	When preparing period ending closing adjustments personnel do not accurately capture all appropriate information. This may result in inaccurate financial statements.	ensure that all journal entries required have been accounted for.			
		At the end of the month the Senior Accountant prints out a listing of manual journal entries from GL and compares it with the journal entry log to ensure that there are no differences.	Automated	Detective	Low
Rights and Obligations – All changes to the Chart of Accounts are approved by Management	Personnel without proper authority add accounts to the general ledger. This unauthorized action may lead to risks affecting accounting transparency. Personnel without proper authority remove accounts from the general ledger. This unauthorized action may lead to risks affecting accounting transparency.	The CFO and Controller approve all changes to the chart of accounts prior to the change being implemented. Only the Controller and Accounting Manager have access to add, change, or delete accounts in the chart of accounts.	Automated	Preventive	Medium
Rights and Obligations – Unauthorized input to general ledger maintenance procedures is prevented and detected.	Personnel without the proper authority have access to the general ledger. This may result in fictitious transactions being process and ultimately financial statement misstatements.	Only the GL Accountant, Senior Accountant, and Accounting Manager have access to opening and closing periods in the General Ledger. The system is password protected and passwords are changed frequently to prevent unauthorized access to general ledger.		Preventive	Medium
Non-recurring transactions			Manual		
Existence and Completeness – All nonrecurring events and transactions are valid and properly recorded in the	Personnel record invalid transactions in the general ledger. This may lead to financial statements coating, misleading, o misstated account balances.	The Corporate Controller reviews details of all nonrecurring transactions for completeness and validity on a monthly basis as part of the monthly journal entry	Automated	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
appropriate accounting period.	Personnel do not record nonrecurring events into the general ledger due oversight. This will lead to incomplete financial statements.	review. The Controller approves the journal entry log and signs this as evidence of review.			
Valuation – All journal entries must balance.	Personnel prepare and enter journal entries into the general ledger which do not balance. This will lead to incomplete, inaccurate financial statements.	The accounting system will not process a journal entry if the entry does not balance. An error message will be displayed for the individual posting the entry to resolve.	Automated	Preventive	Low
Valuation and *Completeness* – Related party events and transactions are identified, appropriately accounted for, and disclosed (if necessary) in the correct accounting period.	Personnel do not adequately identify transactions with related parties. This may lead to inadequate or incomplete disclosure of related party transactions. Personnel do not appropriately account for transactions with related parties. This may lead to incomplete related party information.	A listing of related parties is provided by the CFO, CEO, and Directors to legal department, which compiles the lists and sends it to the Corporate Controller and accounting reporting manager. Reliance is placed on the CFO, CEO, and Directors that the information they provide is complete. The GL accountant performs a search in the AP and AR subledgers to determine transactions with such entities. The GL accountant provides the Controller with the list and the Controller determine if disclosure is appropriate. For Corporate, routine related party activity is reviewed by the Controller on a quarterly basis to ensure disclosure is appropriate.	Manual	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Accruals, Management Estimates, and Reserves			Manual		
Completeness – All accruals and adjustments to reserves are recorded.	Personnel do not properly record a accrual/reserve for existing obligations at the period end date. This may result in understated accrued liabilities. Personnel record inappropriate accruals/reserves for obligations that did not exist at period end. This may result in overstated accrued liabilities.	The Manager monitors accruals and reserves quarterly and confirms information from various sources, such as legal department, marketing, etc., to determine if accrual calculations are appropriate.	Manual	Detective	Low
Existence, Completeness and *Valuation* – Restructuring accruals are appropriately approved and reviewed.	Personnel post journal entries to the general ledger which are not approved by management. This may result in inaccurate or nonexistent restructuring accruals.	Restructuring accruals are initially recorded using detailed plans provided. The restructuring account reconciliations are reviewed by the Corporate Controller monthly to ensure any changes are adequately accounted for, such as subleases, and that the accrual is adequate for estimated future expenses. The Controller reviews a variance analysis, and any significant variances are investigated.	Manual	Preventive	Medium
Valuation and *Completeness* – All nonrecurring events, transactions, classes of transactions, and account balances requiring the use of accounting estimates and the application of judgment are identified and the appropriate accounting treatment is specified.	Personnel make judgments on balance which require accounting estimates without proper review by management. This may result in inappropriate accounting treatment for obligations which existed at period end.	The Controller reviews all balance sheet reconciliations on a monthly basis prior to closing the books. The Controller validates that the accounting treatment is correct and items have been recorded appropriately in the correct accounts and approves any adjusting entries required. The Controller signs the reconciliation as evidence of this review.	Manual	Detective	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Goodwill and Other Intangible Assets			Manual		
Existence, Completeness and *Valuation* – All acquired goodwill and intangible assets are recorded at fair value at acquisition.	Personnel record inappropriate purchase accounting entries which are not detected by management. This may result in inaccurate values of goodwill and intangible assets on the balance sheet. Fair value of goodwill and intangibles are not supported by appropriate analysis and documentation. This may result in over/understatement of goodwill and intangibles in the financial statements.	Acquisition accounting is coordinated by Corporate Accounting to ensure that all balances are recorded at fair value. Independent third-party valuation experts are utilized for material acquisitions. The Controller and CFO review the entries to determine that they are appropriate.	Manual	Preventive	Medium
Existence, Completeness and *Valuation* – Completeness and accuracy of historical data used for evaluating future trends	Financial data provide by acquired company lacks proper financial analysis. This may result in management using inaccurate financial data to perform financial analysis of acquisition target. Management may be in violation of SEC regulations if an independent accounting is not engaged to perform due diligence on significant acquisitions.	Financial analysis is performed by third parties on the historical accounting and financial results of the companies acquired to ensure accuracy and completeness of data considered. Additionally, due-diligence review is performed by an independent public accounting firm if the acquisition is considered significant per the SEC rule.	Manual	Preventive	Medium
Valuation –Validity of handling of acquired debts and obligations	Management does not properly identity valuation risk related to acquired debt obligations. This may result in a lack of risk management strategies to deal with any risks related to debt acquired.	The VP of Finance determines the method for handling any debt obligations and hedging any exchange risks. The CFO approves the strategy.	Manual	Preventive	Medium

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Presentation and Disclosure – Valid and accurate classification of restructuring expenses	Management does not appropriately identify restructuring expenses. This may result incomplete disclosure in the financial statements. Management does not appropriately quantify or apply the appropriate accounting provisions to restructuring expenses. This may result in inaccurate financial statements.	Costs for severance, benefits, payroll taxes, and related charges are accounted for as Restructuring and Other Charges and properly presented and disclosed in the 10-K, 10-Q, and Annual Report.	Manual	Preventive	Medium
Existence, Completeness and *Valuation* – The amortization period for intangible assets represents the period during which the intangible assets are expected to provide value.	Intangibles with an inappropriate useful life are reported on the balance sheet. This may result in an inaccurate carrying value of intangible assets in financial statements. Management does not periodically evaluate intangible assets for impairment even as economic conditions change. This may result in an overstatement of intangible assets in the financial statements.	An independent appraiser determines the useful lives of the assets as part of purchase accounting. The VP of Finance or the Corporate Controller reviews the calculation for reasonableness and approves the applicable useful life.	Manual	Preventive	Low
Existence, Completeness and *Valuation* –Goodwill and intangible asset balances are valid assets, and are systematically tested for impairment on a yearly or more frequent basis.	Goodwill and intangibles which are not tested for impairment on at least a yearly basis may not be carried at the appropriate value on the balance sheet. This may lead to inaccurate goodwill and intangible balances and incomplete disclosure of impairment in the financial statements.	The accounting manager tests goodwill for impairment on an annual basis or when events suggest that a loss in value has occurred. The Controller and CFO approve any adjustments to the financial statements.	Manual	Detective	Medium
Existence, Completeness and *Valuation* – Amortization of intangible assets is recorded in the appropriate period.	Personnel recorded inappropriate amortization expense related to intangible assets. This will result in an incorrect carrying value of the intangible asset in the financial statements.	The GL Accountant calculates and records the amortization expense based on the useful life of the asset. The Controller reviews the amortization and the balance as part of his reconciliation review.	Manual	Detective	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Period Close					
Existence – Postings to prior periods are restricted.	Personnel make adjustments to closed accounting periods. Unauthorized closings entries in prior periods may result in misstated account balances.	Postings to closed periods in Accounting are restricted.	Manual	Preventive	Low
Existence, Completeness and *Valuation* – Reconciliations are properly performed and reviewed for all significant accounts on a timely basis and in the appropriate accounting period; issues identified are resolved.	Personnel do not perform reconciliations in the appropriate accounting period. This may result in inaccurate or incomplete financial statements.	The controller reviews each month all reconciliations prepared in the department. This review considers whether the account was reconciled within 15 days of month-end and whether all unreconciled differences have been resolved.	Manual	Detective	Medium
Existence, Completeness and *Valuation* –Postings from subledger to GL are made completely, accurately, and in the proper period.	Automatic subledger to GL postings are made inaccurate or incomplete. This may result in inaccurate or incomplete financial statements.	The subledger automatically summarizes and posts appropriate entries to the general ledger accounts. The Accounting Manager ensures that subledger is posted accurately as part of the subledger reconciliations.	Automated	Detective	Low
Existence, Completeness and *Valuation* –Suspense, invalid, or other rejected or improper automated postings are analyzed and resolved on a timely basis.	Unresolved suspense, invalid or other rejected or improper automated postings at period end will result in inaccurate financial information in the general ledger. This may result in inaccurate financial reporting.	The Controller reviews and approves all subledgers to general ledger reconciliations on a monthly basis; exceptions are resolved by the senior accountant prior to close. Any suspended or invalid data would show up as a reconciling item.	Manual	Detective	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Foreign Currency Translation			Manual		
Valuation – Exchange rates used to translate foreign currency trial balances or amounts are valid.	Personnel obtain in inaccurate moth end foreign currency rates. This may result in misstated foreign denominated account balances.	Month-end rates used to properly translate balances are obtained by the General Ledger Accountant or Senior Accountant from a reliable third party, such as a government or financial institution website	Manual	Preventive	Low
Valuation – Foreign exchange gains and losses are correctly accounted for.	Personnel may inappropriately recognize gains or losses in the income statement. This may result in inaccurate financial statements.	The Senior Accountant and GL Accountant translate foreign exchange trial balances at the end of the month. Permanent foreign exchange gains and losses are written off in the P&L and are reviewed for appropriateness. Temporary gains and losses are maintained on the balance sheet, which is reviewed and approved by the Corporate Controller as part of the reconciliation process. Refer to SAA.	Manual	Preventive	Medium
Consolidations					
Completeness – All appropriate valid subsidiaries or other applicable organizations are identified and included in the consolidation process.	Personnel fail to identify all subsidiaries which should be included in the company's consolidation. This will result in incomplete financial statements. Personnel inappropriately include subsidiaries in the company's consolidation. This will result in inaccurate financial statements.	Reliance is on the accounting system to include all subsidiaries in the accounts. Management also reviews the monthly financial package and would likely detect unusual amounts in the overall review of the statements	Manual	Detective	Medium
Existence, Rights and Obligations and Valuation – Consolidation	Consolidation packages received from subsidiaries do not accurately reflect the underlying financial records at each	The financial statements submitted for consolidation are prepared from the trial balance that is prepared	Automated	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
packages received from subsidiaries accurately reflect the underlying financial records at each subsidiary.	subsidiary.	directly from the subsidiary's general ledger. All subsidiary financial records are maintained per U.S. GAAP. Statutory adjustments are prepared in the tax returns outside of the ledger.			
Completeness and *Rights and Obligations* – All intercompany transactions and balances are identified, reconciled, and appropriately eliminated in consolidation in the appropriate accounting period.	Personnel do not adequately identify intercompany balances and as such the balances are not eliminated in consolidation. This may result in an overstatement of the financial statements. Personnel do not appropriately reconcile and eliminate intercompany balances. This may result in an overstatement of financial statements.	Intercompany accounts are mainly between subsidiary entities. intercompany reconciliations are approved by the Controller and emailed to the Senior Accountant as evidence of his approval. Only in instances when intercompany accounts do not negate each other does the Senior Accountant access the reconciliations on a shared drive and resolve the issues with counterparts. Access to the shared drive is restricted to finance personnel.	Manual	Preventive	Medium
Presentation and Disclosure – All necessary information from the subsidiaries has been received.	Corporate accounting does not receive complete and accurate financial information from subsidiaries. This may lead to incomplete or inaccurate financial statements. Corporate accounting does not received necessary information subsidiaries required for disclosure. This may result in incomplete and inaccurate disclosure in the financial statements.	One reporting template applies for all subsidiaries that are not in GL. A review is performed by the senior accountant to ensure that forms have been completely filled by the subsidiaries. the subsidiary books close on the 25th, and subsequent activities are captured via a review of the bank statements (main activities are cash related).	Manual	Detective	Medium
Rights and Obligations – Consolidation entries are approved.	Personnel book unauthorized consolidation entries. This may result in inaccurate financial statements.	The Senior Accountant confirms that there are no transactions in suspense in the recovered	Manual	Detective	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
		transactions screen, and prints out a screen shot of the unposted journal log to ensure that there is no suspended/rejected data. The Controller approves all resolutions of suspended/rejected data.			
Completeness and *Presentation and Disclosure* – Inclusion/exclusion of subsidiaries in the consolidation is accurate and is approved by appropriate accounting personnel.	Personnel do not adequately identify subsidiaries and as such the subsidiaries financial information is not included in the consolidation. This may result in inaccurate financial information and disclosures.	Once a subsidiary is acquired, the Controller and CFO together with independent appraisers hold a discussion about the exclusion/inclusion of the subsidiary in the consolidation. Decisions are approved by the Controller and/or CFO based on the independent appraisers' recommendation and are documented appropriately.	Manual	Preventive	Medium
Existence – Inclusion/exclusion of subsidiaries in the consolidation is accurate and is approved.	Personnel do not adequately identify subsidiaries and as such the subsidiaries financial information is not included in the consolidation. This may result in inaccurate financial information and disclosures.	If there is a change in circumstances that would cause a division/subsidiary to be included or not included, the Controller reevaluates the inclusion/exclusion of such subsidiary/division.	Manual	Preventive	Medium
Completeness and Valuation – Consolidation entries are recorded completely and accurately.	Personnel book inaccurate or incomplete consolidating entries. This may result to incomplete or inaccurate financial statements.	The Controller performs a review of the consolidation to verify all consolidated balances are in accordance with U.S. GAAP, after applying elimination entries, and are correct (e.g., intercompany accounts are zero or include just balances due to nonconsolidated related companies). Discrepancies	Manual	Detective	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
		are researched and corrected as necessary by the Senior Accountant.			
Financial Statement Preparation					
All Assertions – Accounting policies are kept current in response to changes in the company's business and operations	Management does not evaluate the impact of changes to the company's business or the overall economic environment in the context of the company's accounting policies. This may lead to misstated financial statements.	Accounting policies for significant transactions are reviewed annually by the Controller for changes in circumstances. Accounting policies are updated as necessary and approved by the Controller and CFO.	Manual	Detective	Medium
All Assertions – All transactions are consistent with established accounting policies	Personnel do not understand or are unaware of the company's accounting policies resulting in deviations from company policy. This will lead to misapplication of the company's accounting policy and potentially misstated financial statements.	All accounting policies and policy changes are communicated to all subsidiaries in a timely manner.	Manual	Preventive	Medium
All Assertions – Interpretation of GAAP requirements is correct	Unqualified personnel are making judgments on interpretations of complex accounting rules without proper guidance from management. This may lead to incorrect application of GAAP and ultimately misstated financial statements.	All decisions regarding policy changes are supported by documentation. The Controller and CFO ensure these are in line with GAAP prior to approval.	Manual	Preventive	Low
All Assertions – Accounting policies are properly approved	Accounting policies are developed by personnel who lack the expertise to interpret complex GAAP. This may lead to the development of accounting policies which are inconsistent with GAAP.	All accounting policies are approved by the CFO and Corporate Controller, and critical accounting policies are approved by the audit committee and are per U.S. GAAP. Accounting policies are updated as needed based on changes in accounting practices.	Manual	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
Presentation and Disclosure – Balances and details are included in the financial statements completely and accurately	Personnel and/or accounting systems do not capture all information from the GL in the financial reporting system. This will result in incomplete financial statement information. Personnel and/or accounting systems capture incorrect information from the GL in the financial reporting system. This will result in inaccurate financial statement information.	Information in the financial reporting system is imported from the accounting system. The Accounting Manager and Senior Accountant reconcile the reporting system to GL. Any discrepancies are investigated and resolved in a timely manner.	Automated	Detective	Low
Presentation and Disclosure –Financial statement information is footed	Financial statements not footed contain computation errors which would lead to inaccurate financial reporting.	The Accounting Manager manually foots financial statements, or utilizes Generalized Audit Software to test the financial statement mechanical accuracy.	Manual	Detective	Low
Presentation and Disclosure –Distributed financial statements are approved for GAAP compliance	Financial statements which are not approved by senior management for GAAP compliance may be inaccurate or lack proper disclosure.	The Accounting Manager compiles other financial statement information, which, together with basic financial statements, is included in regulatory reports. Any questions about these reports are discussed during the drafting session and changes are made to reflect the correct information in the documents. The filings are verified and approved by the CFO or CEO, audit committee, and board of directors.	Manual	Detective	Low
Presentation and Disclosure –Disclosure information is stated accurately and is consistent with other information within the	Disclosure information which does no include all relevant information within the company may lead to incomplete financial disclosures and misleading financial statements. Disclosure information which is not	Commitments and contingencies footnote, which does not come directly from the G/L or supporting systems, is independently verified by the Accounting Manager, the Controller, and other department	Manual	Detective	Medium

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
company	consistent with information within the company may lead to inaccurate financial disclosures and misleading financial statements.	managers where relevant to ensure completeness and accuracy. Refer to Notes to Financial Statements.			
Presentation and Disclosure –Disclosure information is stated accurately and is consistent with other information within the company	Disclosure information which does not include all relevant information within the company may lead to incomplete financial disclosures and misleading financial statements. Disclosure information which is not consistent with information within the company may lead to inaccurate financial disclosures and misleading financial statements.	Certifications and consents are received from the members of executive staff, audit committee, board of directors, and external auditors as applicable. The VP of Legal ensures that these are adequately received.	Manual	Detective	Medium
Presentation and Disclosure –Disclosure information is complete	Disclosure information which does no include all relevant information within the company may lead to incomplete financial disclosures and misleading financial statements.	A disclosure checklist is completed by Accounting Manager on a standard form every quarter to ensure that all disclosure information is complete. The Accounting Manager ensures that the checklist is up to date. The Controller reviews the checklist for completeness and signs as evidence of this review.	Manual	Preventive	Medium
Presentation and Disclosure –Supporting documentation for SEC filings is maintained	Financial statement information contain in filings for which management does not keep adequate supporting documentation may be unsupportable based on SEC or other regulatory inquiry.	A binder is completed and kept for all filings which contains supporting documents and details.	Manual	Preventive	Low

Financial Statement Assertion [20]	Risk	Process Level Control	Manual/ Automated	Preventive/ Detective	Design Effectiveness
SEC Filings and Other Regulatory Disclosures					
All assertions – All other SEC filing requirements (e.g., proxy and other triggering events that warrant Form 8-K) are met and forms are filed accurately and timely in accordance to the SEC rules and regulations	Regulatory filings which are not filed timely by management may lead to fines by the SEC. Regulatory filings which are not filed accurately by management may mislead investors.	Accounting Manager, VP of Legal, and Disclosure Committee are aware of events that trigger SEC disclosures (e.g., 8-K, etc.) and these individuals are aware of various SEC rules and regulations through continuing education and consultation with outside legal counsel. The SEC Manager receives updates and pronouncements on new regulations from external auditors and outside legal counsel.	Manual	Preventive	Medium

E. ILLUSTRATIVE PROCESS LEVEL MATRIX

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
Order Processing					
Valuation – Price and amount of sales are accurate.	Staff capture an inaccurately reflect the selling price on the invoice.	Prices are verified to authorized price lists or standing data before order is processed.	Preventive	Manual	
		Periodic reviews of master price file information are performed by authorized management.	Preventive	Manual	
		An approved price list is maintained and communicated to sales staff and customers.	Preventive	Manual	
	Either staff, or supporting systems, inaccurately calculate discounts, incentives, etc.	Discounts, incentives, etc. are recalculated and/or confirmed before shipment.	Preventive	Automated	
Occurrence – Only valid orders are fulfilled.	Invalid orders are taken.	Key elements of the order (customer name, address, credit limits, etc.) are verified before an order is processed.	Preventive	Manual	
	Duplicate sales orders are processed.	Sales orders are pre-numbered and sequential order monitored.	Preventive	Automated	
Occurrence – Only valid orders are fulfilled (continued).	Orders are accepted at unauthorized prices or terms unacceptable to management.	Clear statement of criteria developed for sales terms.	Preventive	Manual	
		Documented and enforced procedures for review and approval of sales contracts prior to execution.	Preventive	Manual	

[21] Italicized text refers to financial assertions described in the section *Importance of Financial Reporting Objectives*

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
	Orders are accepted at unauthorized prices or terms unacceptable to management.	Exception reporting procedures report orders that do not meet established criteria.	Detective	Automated	
	Large, unusual or related party orders are fulfilled.	Independent departments review all material sales agreements including finance and legal.	Preventive	Manual	
		Authorization levels are clearly documented and communicated including board approval for related party and high-risk transactions.	Preventive	Manual	
	Unacceptable customers are added to the customer list.	Changes must be approved in writing by specified executive or supervisory employee.	Preventive	Manual	
	Customer list is inaccurate or incomplete.	Periodic review of customer lists for accuracy and completeness including whether they continue to meet the criteria for establishing a customer.	Detective	Manual	
		Written chart of accounts containing a description of each account.	Preventive	Manual	
	Order processing procedures are implemented that circumvent existing internal control techniques.	The entity has established order processing policy and procedure manuals and training routines.	Preventive	Manual	
Completeness – All valid orders are processed and recorded.	Back orders are not fulfilled.	Policy and procedures are in place to log, track and monitor back orders.	Detective	Automated	
		Sales orders are pre-numbered and sequential order monitored.	Preventive	Automated	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
	Orders are not recorded properly.	The entity reconciles subsidiary ledger accounts receivable and sales ledger balances to general ledger balances or other control totals on a regularly scheduled basis.	Detective	Manual	
		Written closing procedures stating, by function, the sources to be used to prepare journal entries, cut-offs to be observed, accruals to be made, and who is responsible to do what.	Preventive	Manual	
		Standard journal entry register or other control to provide reasonable assurance that all required journal entries are prepared.	Detective	Automated	
		Validity checking and/or verification of key data fields of each journal entry.	Detective	Automated	
		Period-to-budget comparisons of amounts of recurring entries.	Detective	Manual	
Presentation and Disclosure – Relevant information is captured and reported accurately and promptly.	Disclosure data is not identified timely.	Early identification of each supplemental disclosure to be made by, 1. Reference to prior-year financial statements 2. Minutes of Board of Directors' and shareholders' meetings	Detective	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
		3. Review of new regulatory pronouncements			
	Disclosure data is not identified by each department.	Assignment of responsibility for gathering the required data to specific individuals.	Preventive	Manual	
	Personnel are provided with inadequate instruction on how to promptly and accurately report disclosure data. As a result, elements of required disclosure data may be omitted.	Written statements of data-gathering procedures to facilitate prompt and accurate reporting.	Preventive	Manual	
Rights and Obligations – Only appropriate users can enter sales orders.	Lack of segregation of duties.	Access levels are pre-defined based on clear job responsibility.	Preventive	Automated	
		Independent review by management.	Detective	Manual	
	Inappropriate access by unauthorized personnel.	Restricting order input by the use of passwords.	Preventive	Automated	
Distribution and Delivery					
Valuation – Correct goods are shipped and accurately recorded.	Incorrect items are included or substituted in the order.	Order is verified or confirmed against customer request before delivery.	Preventive	Manual	
Existence – Deliveries are recorded in the proper period.	Backlog orders are not properly monitored.	Unfulfilled orders are monitored on a regular basis.	Detective	Manual	
Completeness – All deliveries are recorded.	Inventory is incorrectly recorded.	Periodic physical inventories of stocks of critical forms and reconciliation to controls.	Detective	Manual	
	Inventory is incorrectly recorded.	Maintenance of logs at stocking locations, which may be used to: - accrue production as of activity dates rather than processing dates and/ - check the completeness of registers and journals.	Detective	Automated	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
Existence – Sales are recorded in the proper period.	Deliveries are recorded prematurely or in the incorrect period.	Delivery activities are reconciled to sales on a regular and frequent basis.	Preventive	Manual	
Completeness - All work orders or shipments of goods are input for processing.	Work orders are incomplete or missing.	Work orders are pre-numbered and monitored.	Preventive	Automated	
Valuation – Postings made to cost of sales and/or inventory in the general ledger are correct.	Human error in coding or entry.	Independent reconciliation of accounts.	Detective	Manual	
Rights and Obligations – Only appropriate users can enter delivery of goods.	Inappropriate access to delivery systems.	Access levels are pre-defined based on clear job responsibility.	Preventive	Automated	
	Inadequate segregation of duties.	Independent review by management.	Detective	Manual	
Cash Receipts			Preventive Detective	Manual Computer	
Valuation – Cash receipts are accurately recorded.	The amount of cash receipts are inaccurately recorded.	Correct recordings are confirmed by independent personnel.	Preventive	Manual	
	Cash receipts are recorded in the improper period.	Documented processing, cut-off, and period-end closing procedures.	Preventive	Manual	
	Cash receipts do not relate to sales and/or are not recorded against the correct customer or invoice.	Reconciliation of subsidiary ledger accounts receivable and sales ledger balances to general ledger balances or other control totals on a regularly scheduled basis.	Detective	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
	Cash receipts are not input for processing.	The entity performs batching and reconciling input totals to processing totals and new balances forwarded.	Preventive	Automated	
	Periodic updates for batch processing are inappropriately executed.	Supervisory or managerial personnel review periodic updates.	Detective	Manual	
	Bank statements are inconsistent with general ledger accounts.	The entity has processes in place to regularly reconcile bank statements and general ledger accounts.	Detective	Manual	
	The entity's bank statements are inconsistent with that recorded by the bank.	The entity has processes in place to regularly reconcile recorded balances and activities with balances and activities reported by its banks.	Detective	Manual	
	Inappropriate access to receive and record cash receipts.	Access levels are pre-defined based on clear job responsibility.	Preventive	Automated	
Valuation – Cash receipts are accurately recorded (continued).	Inadequate segregation of duties.	Independent review by management.	Detective	Manual	
	Cash receipts are not protected before they are deposited.	Cash receipts are stored in a manner which protects them from physical destruction or manipulation. Backups of cash receipts are made.	Detective	Manual	
Valuation – Timely collection of accounts receivable is monitored.	Doubtful accounts have not been appropriately identified and considered.	Accounts receivable aging reports are prepared regularly and analyzed by management.	Detective	Manual	
		Customer open items reports are prepared and analyzed by management.	Detective	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
Existence – Cash receipting function is periodically reviewed for compliance with entity policy.	Cash receipting function is periodically not in compliance with entity policy or presents risks to the entity.	Periodic internal audits.	Detective	Manual	
Existence – Cash receipts are recorded in the period in which they are received.	Cash receipts are not recorded in the period in which they are received.	Cash sales are recorded using a cash register. Customers are provided with the register receipt and total daily receipts per the register are balanced to cash deposited to the bank.	Detective	Manual	
Presentation and Disclosure – Relevant disclosure data is gathered accurately and promptly.	Disclosure data is not identified by each department.	Assignment of responsibility for gathering the required data to specific individuals.	Preventive	Manual	
	Personnel are provided with inadequate instruction on how to promptly and accurately report disclosure data. Elements of required disclosure data may be omitted.	Written statements of data-gathering procedures so the data can be reported promptly and accurately.	Preventive	Manual	
Invoicing					

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
Rights and Obligation – Recorded balances of accounts receivable, and related transaction activity, are periodically substantiated and evaluated.	Inadequate guidance exists for proper recording of accounts receivable.	Policy statements, procedures manuals, organization charts, and/or other documentation that: - List the balances, reports, activities, policies, and procedures that are to be substantiated and evaluated, when they are to be substantiated and evaluated, and by whom the activity will be supervised - Describe how the substantiation and evaluation should be performed - Describe how the results of the review should be documented and to whom they should be communicated.	Preventive	Manual	
Existence – Recorded balances of accounts receivable, and related transaction activity, are periodically substantiated.	Records of accounts receivable are inadequate.	Comparison of recorded amounts of reserves, liabilities, and accruals with subsequent transactions.	Detective	Manual	
		Analysis of key ratios, trends, and variances.	Detective	Manual	
Existence – Invoices are recorded in the appropriate period.	Invoices are not recorded in the appropriate period.	Goods shipped at, before, or after the end of an accounting period are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period including the raising and recording of the related invoices.	Detective	Manual	
Valuation – The price and amount of sales are accurate.	Formulae used for calculating accounts receivables entries are inaccurate.	Periodic reviews of formulae used for accruals, write-offs, etc.	Detective	Manual	
	Selling price is inaccurate.	Prices are verified to authorized	Preventive	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
.		price lists or standing data before invoice is issued.			
	Selling price is inaccurate.	Periodic reviews of master prices file information are performed by authorized management.	Preventive	Manual	
	Inaccurate price lists are used.	An approved price list is maintained and communicated to sales staff and customers.	Preventive	Manual	
	Selling price is inaccurate.	Comparisons are made of actual results with budgeted results and analyses of variances.	Detective	Manual	
	Discounts, incentives, etc. are calculated incorrectly.	Discounts, incentives, etc. are recalculated and/or confirmed before invoice is issued.	Preventive	Manual	
	Discounts, incentives, etc. are calculated incorrectly.	Comparisons are made of actual results with budgeted results and analyses of variances.	Detective	Manual	
	Customer complaints regarding inaccurate bills are not investigated or monitored.	Policies and procedures in place to handle and track customer billing complaints.	Detective	Manual	
Completeness – A sales invoice is generated for every shipment or work order.	Delivery slip or work order is lost or missing.	Bill of lading/delivery slips are pre-numbered and sequential order monitored.	Preventive	Automated	
	Deliveries are made but not recorded.	Comparisons are made of actual results with budgeted results and analyses of variances.	Detective	Manual	
	Invoices are not sent out properly.	Assignment of responsibility for each account balance to a particular individual in the cycle	Preventive	Manual	
Rights and Obligations – Only appropriate users can generate sales invoices.	Inadequate segregation of duties.	Independent review by management.	Detective	Manual	
		Rotation of bookkeepers among various ledgers.	Preventive	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
	Invoicing function is periodically not in compliance with entity policy or presents risks to the entity.	Periodic internal audits.	Detective	Manual	
Credit Notes and Adjustments					
Existence – Credit notes issued are recorded in the appropriate period.	Goods returned by customers are not recorded in the appropriate period.	Goods returned by customers at, before, or after the end of an accounting period are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period.	Detective	Manual	
Valuation – Credit notes and adjustments to accounts receivable are accurately calculated and recorded.	Credit notes and adjustments to accounts receivable are not accurately calculated and recorded.	Management approves credit notes, bad-debt write-offs, and other adjustments to accounts receivable.	Preventive	Manual	
		Management monitors the nature, volume and amount of recorded credit notes, write-offs, and other adjustments to accounts receivable.	Detective	Manual	
Completeness – All credit notes and adjustments to accounts receivable are recorded.		All returned goods are logged when received. The log details items such as customers, goods, defects, inspections and assessment by quality control. Return details per the log are compared to credit notes issued to ensure that credit is issued in the correct period and in accordance with company policy.	Preventive	Automated	
Information Technology					
Completeness – A sales invoice is generated for every shipment or work order.	Order data is not transferred completely from the order entry subsystem to the invoicing subsystem.	Data transferred from the order entry subsystem to the invoicing subsystem is balanced; identified errors are corrected promptly.	Preventive	Automated	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
Valuation –Invoice are generated using authorized terms and prices	Data input into the invoicing system is inaccurate compared to the order entry system.	Data input to the invoicing system is compared to priced order and shipment data per the separate, nonintegrated order entry and/or shipping applications; differences require management approval before invoices can be processed.	Preventive	Automated	
Completeness and *Valuation* – All changes to standing data are completely and accurately inputted.	Human error causes changes to standing data to be incompletely and inaccurately inputted.	Independent review by management.	Detective	Manual	
	Periodic updates for batch processing are improperly executed.	Process for executing batch processing triggers a review of standing data.	Detective	Automated	
	Inappropriate access to customer and price information and lack of segregation leads to inappropriate employee behavior.	Access levels are pre-defined based on clear job responsibility.	Preventive	Automated	
	The process for approving changes to standing customer information, account codes, and credit limits is insufficient.	The process for approving changes is documented and followed. The process includes review by senior personnel.	Preventive	Manual	
	The process for approving changes to price lists approved is insufficient and leads to a price list which is not aligned with management's strategy or the entity's cost basis.	The process for approving changes is documented and followed. The process includes review by senior personnel.	Preventive	Manual	
Completeness and *Valuation* – All changes to standing data are completely and accurately inputted (continued)	The process for approving changes to price lists approved is insufficient and leads to a price list which is not aligned with management's strategy or the entity's cost basis.	Requests to change customer master file data are submitted on prenumbered forms; the numerical sequence of such forms is accounted for.	Preventive	Manual	

Financial Statement Assertion [21]	Risk	Process Level Control	Preventive / Detective	Manual / Automated	Design Effectiveness
	The process for approving changes to price lists approved is insufficient and leads to a price list which is not aligned with management's strategy or the entity's cost basis.	Recorded changes to customer master file data are compared to authorized source documents or confirmed with customers to ensure that they were input accurately.	Detective	Manual	

F. METHODOLOGY

Background

In January 2005, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project, designed to help smaller organizations implement COSO's *Internal Control – Integrated Framework (Framework)*. This initiative will fill a gap in existing guidance and help smaller companies reach compliance with laws and regulations pertaining to internal control over financial reporting. PricewaterhouseCoopers was engaged to conduct this project, resulting in this report, *Internal Control – Integrated Framework: Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting.*

The *Framework* has been widely accepted as the internal control over financial reporting standard for organizations implementing and evaluating internal control in compliance with the U.S. Sarbanes-Oxley Act of 2002 and U.S. Public Company Accounting Oversight Board (PCAOB) Standard 2. Smaller companies have unique challenges regarding compliance with Sarbanes-Oxley Section 404 requirements and are seeking guidance that will help them understand the breadth, depth, and value of COSO's *Framework* as they go through the process of evaluating internal control over financial reporting. The guidance provided by this project is not intended to replace or modify the *Framework*, but rather demonstrates the *Framework's* broad applicability by providing concrete examples that smaller businesses can use to achieve their financial reporting objectives.

Project Structure

Input was obtained from corporate executives of many smaller organizations. Executives included chief executive officers, chief financial officers, controllers, and internal auditors; others who provided input include investors, legislators, regulators, lawyers, external auditors, consultants, and academicians.

Throughout the project, the project team received advice and counsel from an Advisory Task Force reporting to the COSO Board. The Task Force consisted of approximately twenty members with experience in small business, a PricewaterhouseCoopers research team all experienced in small business, and the COSO board members. The Task Force held a forum in May with invitees from small businesses to better understand the unique challenges those businesses face in developing and implementing controls. Task Force leaders and board members attended the SEC Commission Roundtable on Internal Control Reporting Requirements in April that solicited input on Sarbanes-Oxley Section 404. Various drafts of this guidance have been reviewed by individuals working with, or for, smaller businesses. Finally, preliminary versions of this guidance, especially the principles contained herein, have been presented to groups such as the AICPA's major firm group – a group of fifty of the largest public accounting firms (other than the "Big Four") that

specialize in working with smaller businesses. There was support in the group for the principles-based approach to assist companies in implementing the *Framework*.

At important project milestones, the Task Force and the project team communicated with the COSO Board.

Approach

The project consisted of four phases:

- **Research** – This phase identified, through literature reviews and public forums, current challenges facing smaller businesses when implementing the *Framework*. In this phase, the team analyzed information, contrasted approaches, and identified critical issues and concerns.
- **Building and Designing –** The team developed the guidance, including principles, attributes, approaches, and examples. The guidance was reviewed with key user and stakeholder groups, and reactions and suggestions for enhancement were obtained.
- **Preparation for Public Exposure –** In this phase, the team refined the guidance through review with several companies. The Task Force also considered whether the guidance was sound, logical, and useful to management of smaller businesses.
- **Finalization –** This phase encompassed issuing the guidance for public exposure for a 60-day comment period. Upon receipt of comments, the Task Force reviewed and analyzed them, and identified any needed modifications. The team then finalized the guidance and provided the final guidance to the COSO Task Force and COSO Board for review and acceptance.

As one might expect, many different and sometimes contradictory opinions were expressed on fundamental issues – within a project phase and between phases. The project team, with COSO Task Force and Board oversight, carefully considered the merits of the positions put forth, both individually and in the context of related issues, embracing those that facilitated development of a relevant, logical, and internally consistent document.

Acknowledgments

The COSO Board, Task Force, and PricewaterhouseCoopers LLP gratefully acknowledge the many executives, legislators, regulators, auditors, academics, and others who gave their time and energy to participating in and contributing to various aspects of the study. Also recognized are the considerable efforts of the COSO organizations and their members who participated in workshops and meetings, and provided comments and feedback throughout the development of this guidance.

Many other PricewaterhouseCoopers partners and staff provided important input to this framework, including Myra Cleary, Carlo di Florio, Chris Fox, Robert Fish, and Lisa Tassinari.