



**Internal Control —  
Integrated Framework**

**Guidance on Monitoring  
Internal Control Systems**

**September 2007**

**Discussion Document**

Public Comment Period  
Closes October 31, 2007

## Committee of Sponsoring Organizations of the Treadway Commission

### Board Members

**Larry E. Rittenberg**  
COSO Chair

**Mark S. Beasley**  
American Accounting Association

**Charles E. Landes**  
American Institute of Certified Public  
Accountants

**Edith G. Orenstein**  
Financial Executives International

**David A. Richards**  
The Institute of Internal Auditors

**Jeffrey Thomson**  
Institute of Management Accountants

## Grant Thornton LLP — Author

### Principal Contributors

**James P. Burton**  
Partner  
Grant Thornton LLP — Denver

**J. Russell Gates**  
President  
Dupage Consulting LLC — Chicago

**R. Trent Gazzaway** (Project Leader)  
Partner  
Grant Thornton LLP — Charlotte

**Keith O. Newton**  
Partner  
Grant Thornton LLP — Chicago

**Sridhar Ramamoorti**  
Partner  
Grant Thornton LLP — Chicago

**Richard L. Wood**  
Partner  
Grant Thornton LLP — Toronto

**R. Jay Brietz**  
Senior Manager  
Grant Thornton LLP — Charlotte

### Review Team

**Andrew D. Bailey Jr.**  
Senior Policy Advisor  
Grant Thornton LLP — Phoenix

**Dorsey L. Baskin Jr.**  
Partner  
Grant Thornton LLP — Dallas

**Craig A. Emrick**  
VP - Senior Accounting Analyst  
Moody's Investors Service

**Philip B. Livingston**  
Vice Chairman, Approva Corporation  
Former President and CEO,  
Financial Executives International

## COSO Task Force

**Abraham D. Akresh**  
Senior Level Expert for Auditing  
Standards  
U.S. Government Accountability  
Office

**Douglas J. Anderson**  
Corporate Auditor  
Dow Chemical Company

**Robert J. Benoit**  
President and Director of SOX Research  
Lord & Benoit, LLC

**Richard D. Brounstein**  
Executive Vice President,  
Calypte Biomedical Corporation  
Director, The CFO Network

**Jennifer M. Burns**  
Partner  
Deloitte & Touche LLP

**James W. DeLoach**  
Managing Director  
Protiviti

**Miles E. Everson**  
Partner  
PricewaterhouseCoopers LLP

**Audrey A. Gramling**  
Associate Professor  
Kennesaw State University

**Scott L. Mitchell**  
Chairman and CEO  
Open Compliance & Ethics Group

**James E. Newton**  
Partner  
KPMG LLP

**John H. Rife**  
Partner  
Ernst & Young LLP

**Michael P. Rose**  
CEO and Senior Partner  
GR Consulting LLP

**Robert S. Roussey**  
Professor of Accounting  
University of Southern California

**Sabrina L. Springfield**  
Assistant Director  
U.S. Government Accountability  
Office

**Andre Van Hoek**  
Vice President, Corporate Controller  
Celgene Corporation

## Observers

### Securities and Exchange Commission

**Josh K. Jones**  
SEC Observer  
Professional Accounting Fellow

**Michael G. Gaynor**  
SEC Observer  
Professional Accounting Fellow (former)

## From the Chairman ...

The COSO board believes that the monitoring component of a properly designed and functioning internal control system — utilizing COSO’s *Internal Control – Integrated Framework* — has often been underutilized by organizations of all sizes. This discussion document, which is the first phase of our broader monitoring project, is intended to improve the understanding of the building blocks of effective monitoring, thereby improving both the efficiency and the effectiveness of the entire system of internal control. The guidance presented is effective for all three internal control objectives, including the financial reporting objective that is relevant to public reporting under the Sarbanes-Oxley Act of 2002 or under similar regulatory initiatives around the world.

Introduced in 1992 as one of the five fundamental components of the Framework, monitoring is designed to “ensure that internal control continues to operate effectively.” COSO’s 2006 internal control guidance for smaller public companies elaborates further on monitoring by emphasizing two fundamental points:

- Monitoring should be designed to determine whether all components of internal control continue to operate effectively; and
- Weaknesses in internal control should be communicated in a timely fashion to those responsible (including management and the board) such that corrective action can be taken.

Monitoring is therefore an integral part of internal control. Further, it is important that internal control is viewed as a continuous process and that effective monitoring is implemented as a component of that process — whether that control process applies to operations, compliance, or financial reporting activities.

The second phase of the monitoring project, scheduled for release after comments are received on this discussion document, will provide examples, case studies, and tools to assist all organizations in implementing effective and efficient monitoring. Our intent is to release an exposure draft of the full implementation guidance later this year and to release the final guidance in the first quarter of 2008.

COSO seeks your feedback on the concepts in this discussion document — we want to know if they are clearly articulated and if you agree with the conclusions reached. We also want to receive examples of innovative approaches you have taken in monitoring the effectiveness of internal control. We have developed an online comment form for you to complete and will consider your observations in the development of our final guidance. A link to the form is located at [www.coso.org/publications.htm](http://www.coso.org/publications.htm). Please submit your comments by October 31, 2007.

I would like to recognize the major contribution of Grant Thornton LLP and its team in leading this project. In particular, I want to thank Trent Gazzaway for his yeoman’s efforts in pushing the project forward and leading discourse on very difficult concepts. Through many hours of exchange and debate, the project team, task force, and COSO board dealt with numerous challenges in developing this discussion document.

I also want to recognize and thank all members of the task force listed inside the front cover. Each of them made a significant contribution to the process that yielded this guidance — challenging us to be crisp in our definitions and providing examples of their companies or clients who have implemented effective monitoring of internal control.

As Chair of COSO, I extend my thanks to the five sponsoring organizations for their continued support and contributions to the task force: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

We look forward to your comments.

**Larry E. Rittenberg, PhD, CPA, CIA**  
Chair, COSO



Executive Summary	i
<b>I. Monitoring as a Component of Internal Control Systems</b>	<b>1</b>
Role of Monitoring	1
Structure of Effective Internal Control Systems	3
Difference Between Monitoring Activities and Control Activities	5
<b>II. Fundamentals of Monitoring</b>	<b>5</b>
Attributes of Ongoing Monitoring and Separate Evaluations	6
Attributes of Effective Communication and Follow-Up	7
Elements of Effective Monitoring	7
Role of the Board/Audit Committee	10
<b>III. Nature of Information Used in Monitoring</b>	<b>11</b>
Information Suitability	12
Information Sufficiency	16
<b>IV. Designing Effective Monitoring</b>	<b>18</b>
Prioritizing and Designing Monitoring Procedures	18
Deciding When and How Often to Monitor	24
<b>V. Communicating and Addressing the Results of Monitoring</b>	<b>25</b>
Ranking Issues and Reporting Internally	25
Reporting to External Parties	27
<b>VI. Scalability of Monitoring</b>	<b>28</b>
Scalability Based on Size	28
Scalability Based on Complexity	29
Formality of Monitoring and Level of Documentation	30
<b>VII. Conclusion</b>	<b>30</b>
Appendix: Principles of Effective Internal Control Over Financial Reporting	A-1
Glossary	Glossary-1



## Executive Summary

Internal control systems exist to help organizations meet their goals and objectives. They enable management to deal with changes in internal and external environments. They also promote efficiency, reduce the risk of loss, and help ensure financial statement reliability and compliance with laws and regulations.<sup>1</sup>

Internal control is, therefore, critical to the success of any organization. When it is effective, management and the board have **reasonable assurance**<sup>2</sup> regarding achievement of an organization's goals and objectives. When it is not effective, neither management nor the board has such assurance. It follows, then, that organizations need a mechanism for assessing the quality of their internal control systems' performance over time. That mechanism is monitoring.<sup>3</sup>

Effective monitoring helps ensure that internal control continues to operate effectively. It involves assessment by appropriate personnel of the design and operation of controls on a suitably timely basis, and the taking of necessary actions.<sup>4</sup> These concepts are summarized in two fundamental principles:<sup>5</sup>

- Ongoing monitoring and/or separate evaluations enable management to determine whether the components of internal control<sup>6</sup> continue to function over time.
- Internal control weaknesses should be identified and communicated in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate.

These principles and the concepts behind them are clearly supported by the COSO Framework (notably in the Executive Summary, Chapter 1, and Chapter 6) and by COSO's 2006 Guidance, Chapter V. This discussion document is designed to further develop the understanding of effective monitoring so that organizations can (1) recognize and properly utilize effective monitoring where it exists, and (2) implement effective monitoring where it is needed.

---

<sup>1</sup> See The Committee of Sponsoring Organizations' 1992, *Internal Control — Integrated Framework* (the COSO Framework), pp. 3, 13.

<sup>2</sup> See Glossary for definitions of terms set in boldface.

<sup>3</sup> See the COSO Framework p. 69.

<sup>4</sup> Ibid.

<sup>5</sup> See COSO's 2006, *Internal Control over Financial Reporting — Guidance for Smaller Public Companies* (COSO's 2006 Guidance), Chapter V.

<sup>6</sup> The COSO Framework identifies five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring.

Monitoring is most likely to achieve its purpose through the mutually dependant characteristics of effectiveness and efficiency. Over time, *ineffective* monitoring leads to control breakdowns, which reduce the efficiency of the entire internal control system. Likewise, *inefficient* monitoring may limit an organization's ability to focus finite resources in the areas of greatest risk, thus reducing its effectiveness.

Three primary elements of monitoring influence its effectiveness and efficiency:

1. The control environment in which monitoring operates;
2. The organization's ability to prioritize effective monitoring procedures and devote monitoring resources commensurate with the underlying level of risk; and
3. The organization's communication structure and its ability to report results of monitoring, including control weaknesses, to the right people in a timely manner.

These elements and their effect on monitoring are discussed throughout the remainder of this discussion document.

### **Control Environment for Monitoring**

An effective control environment for monitoring includes (1) a proper tone at the top regarding the importance of monitoring and (2) an organizational structure that places people (i.e., evaluators) with appropriate skills and authority in monitoring roles.

Organizations establish a proper tone at the top by communicating expectations to evaluators regarding the importance of internal control and the related role of monitoring — namely, that monitoring throughout the organization is expected to:

- Support reasonable conclusions regarding the continued effectiveness of internal control, and
- Identify and correct control weaknesses before they materially affect the organization's objectives.

Organizations begin the process of meeting these expectations by placing **competent** and **objective** people in monitoring roles throughout the organization. *Competence* refers to an evaluator's knowledge of the controls and related processes, including how controls should operate and what constitutes a control weakness. *Objectivity* relates both to the way in which information is generated for use in monitoring and to the characteristics of evaluators. Objective individuals provide information and/or perform monitoring procedures with no concern about possible personal consequences and no vested interest in manipulating the information for personal benefit or self-preservation.

## **Prioritizing Effective Monitoring Procedures**

To develop effective and efficient internal control systems, management identifies and evaluates risks to achieving the organization's objectives. This exercise, ordinarily performed in the risk assessment component of the COSO Framework, allows management to respond to risks by designing and implementing appropriate controls. The information gathered in the risk assessment process, and the conclusions about the significance and likelihood of various risks, influence the scope of monitoring (i.e., what is monitored, by whom, using what procedures, and how often). Factors that might have a broad impact on the scope of monitoring include:

- The size and complexity of the organization;
- The nature of the organization's operations (i.e., the degree to which those operations are subject to significant change or to high-risk activities such as fraud);
- The purpose for which monitoring is being conducted (e.g., for internal operational purposes versus external regulatory purposes); and
- The relative importance of the underlying controls in meeting the organization's objectives.

Effective internal control systems lose their effectiveness when (1) processes or risks change, and the underlying controls do not adapt, or (2) previously effective controls cease to operate as they were designed. In either case, the risk inherent in any effective internal control system is that change is not properly identified and managed.

One way organizations can prioritize monitoring with an appropriate risk-based focus is through a structure that first establishes that internal control is effective in a given area and then — for some reasonable period of time — focuses monitoring attention on areas of change. Such a structure might be similar to the following:

1. A Control Baseline — Providing a reasonable basis for believing that internal control in a given area operates effectively, thus establishing a suitable starting point for more-efficient monitoring.
2. A Change-Identification Process — Identifying changes in (1) processes or risks that may indicate that controls should have changed, or (2) the operation of controls that might impact their ability to meet their intended objective.
3. A Change-Management Process — Verifying that, to the extent existing controls are changed or new controls are implemented, the internal control system manages them appropriately. This process also establishes a new control baseline.
4. Control Reconfirmation — When necessary, periodically reconfirming control operation through appropriate separate evaluations.

Regardless of the structure employed, effective monitoring involves gathering and analyzing appropriately **persuasive information** to support conclusions about the effectiveness of internal control. Section III of the discussion document describes in detail the nature of persuasive information, namely its **suitability** and **sufficiency**; however, one key aspect of persuasive information — the difference between direct and indirect information — deserves special mention here.

**Direct information** clearly substantiates the operation of controls. It is obtained by observing controls in operation, reperforming them, or otherwise directly testing their operation. Direct information provides an unobstructed view of control operation. As such, it provides the primary support for the control baseline discussed above, and it provides the most dependable source of support for control conclusions throughout the monitoring process.

**Indirect information** is all other information used to assess whether controls or control components continue to operate effectively, and includes data that either relates to or comes out of the process in which the controls reside. Examples include, but are not limited to, operating statistics, **key risk indicators**, **key performance indicators** or, possibly, comparative industry metrics.

Indirect information seeks to identify anomalies that *might* indicate that a control, or set of controls, failed to operate effectively. The absence of such anomalies, however, does not demonstrate explicitly to evaluators that underlying controls are operating effectively. Rather, monitoring procedures that utilize indirect information can provide additional support for conclusions reached through other monitoring procedures, possibly extending the period of time between separate evaluations using direct information.

### **Communication Structure for Monitoring**

Monitoring is effective only to the extent that results are reported to the appropriate people and corrective action is taken, if necessary. Accordingly, the results of monitoring should be reported to supervisors and/or to executive management in a reasonable time frame. To whom and how often the general results of monitoring are reported depends on the level of risk and the importance of the related controls.

Identified control weaknesses, however, should be reported to the person responsible for the control's operation and to at least one level higher. Reporting at least to these two levels gives the responsible person the information necessary to correct control operation and also helps ensure that appropriately objective people are involved in the severity assessment.

Some organizations assess severity along a continuum such as high, medium, or low, or along a numerical scale (e.g., 1–5 or 1–10). Regardless of the scale used, the two factors that most influence the final ranking are “likelihood” and “significance.” In the context of ranking identified control weaknesses, likelihood is the probability that a control will fail to detect or prevent a risk’s occurrence, and significance is the potential impact of the risk if it occurs.

Appropriately assessing the severity of control weaknesses, and reporting them in a timely fashion to the right organizational levels for possible correction, achieve the highest goal of monitoring — which is to protect the organization and preserve its ability to achieve its objectives.



## I. Monitoring as a Component of Internal Control Systems

In 1992, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed its *Internal Control — Integrated Framework* (the COSO Framework) consisting of five interrelated and equally important components. Four components relate to the design and operation of the system of internal control: control environment, risk assessment procedures, control activities, and information and communication. The fifth component — monitoring — is designed to “ensure that internal control continues to operate effectively.” This discussion document provides guidance for any organization regarding the design and execution of effective and efficient monitoring procedures.

### Role of Monitoring

In an effective internal control system, the COSO Framework’s five components work together, providing **reasonable assurance**<sup>7</sup> to management and the board of directors<sup>8</sup> regarding the achievement of the organization’s objectives.<sup>9</sup> The effective operation of the monitoring component enables management and the board to determine whether the internal control system — which includes all five components — continues to operate effectively over time. It also promotes good control operation through oversight.

Monitoring is effective when it leads to the identification and correction of control weaknesses *before* they **materially** affect the achievement of the organization’s objectives. For example, monitoring should be designed to identify and correct weaknesses in internal control over financial reporting before they can result in a material misstatement of an organization’s published financial statements. In an operational setting, monitoring should be expected to identify and correct

#### 1992 COSO Framework

“Monitoring ensures that internal control continues to operate effectively. This process involves assessment by appropriate personnel of the design and operation of controls on a suitably timely basis, and the taking of necessary actions. It applies to all activities within an organization, and sometimes to outside contractors as well.”

<sup>7</sup> See Glossary for definitions of terms set in boldface.

<sup>8</sup> Many organizations have boards of directors and related board committees to help oversee the conduct of their activities. Other organizations may not have a formal board of directors, but may have other stakeholders who serve in a governance and oversight capacity. For simplicity, this discussion document will use the terms “board of directors” or “board” to refer to all groups charged with governance and management oversight.

<sup>9</sup> COSO Framework, p. 15.

weaknesses in controls over a manufacturing process before they lead to the production and sale of defective goods.

Just as the presence of effective monitoring helps ensure and promote good internal control operation, a lack of effective monitoring leads eventually to deteriorating internal control systems. Internal controls within any or all of the five components may change or cease to be performed, or the circumstances for which controls were created may change, rendering them less effective or ineffective.

No system of internal control can guarantee that all control weaknesses that may result in material errors<sup>10</sup> will be prevented and detected. However, effective monitoring programs will help ensure that internal control continues to operate effectively.

The scope (i.e., the type, timing and extent) of monitoring necessary to support conclusions about a system's effectiveness varies depending on the circumstances. The risk-assessment component of internal control<sup>11</sup> provides the information necessary to make those determinations. In any case, the level of effort in monitoring should be proportionate to the importance of the underlying controls.

Some variables to consider in the risk assessment process, which are discussed further in this document, include the size and complexity of the organization, the nature of an organization's operations, the purpose for which monitoring is being conducted, and the relative importance of the underlying controls in meeting the organization's objectives.

The process of effective monitoring requires thoughtful planning and the evaluation of **persuasive information** to support conclusions regarding the effectiveness of the internal control system. Monitoring must become part of an organized effort that goes beyond simple observation of operations. It should be designed to provide evidence that:

- The internal control system remains effective, both in its current operation and in its ability to respond to changes in relevant risks; and
- Control weaknesses are analyzed, and appropriate follow-up actions are taken that address root causes.

---

<sup>10</sup> Throughout this discussion document, the term "error" refers to the effect of internal control failures. Failures can be intentional (i.e., fraud) or unintentional, and jeopardize the organization's objectives.

<sup>11</sup> See COSO Framework, p. 4, and Chapter 3.

## Structure of Effective Internal Control Systems

The COSO Framework states that:

Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.<sup>12</sup>

Organizations achieve these objectives through the operation of the five interrelated components of internal control, which are inherent in the way management runs the enterprise. The five components are linked and serve as criteria for determining whether the internal control system is effective.

The concepts embodied in the COSO Framework are frequently presented in terms of a three-dimensional cube (Figure 1) that depicts the five components operating *across* each internal control objective<sup>13</sup> and *within* all organizational units and activities.



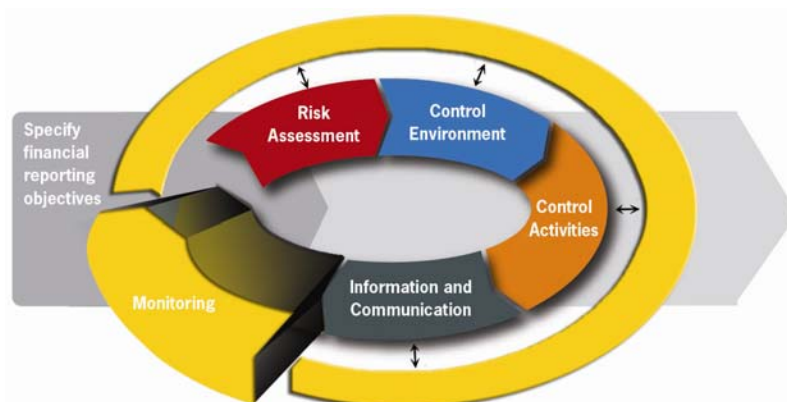
The COSO Internal Control Integrated Framework  
**Figure 1**

The cube not only demonstrates the connections between objectives and components, it also illustrates that the control components operate at different levels across the organization — a concept that is often overlooked. Like the other control components, monitoring can operate at different levels. As organizations increase in size, **evaluators** at the highest organizational levels — who are removed from direct interaction with control components or process owners — often monitor by evaluating the results from lower-level monitoring. Conversely, in smaller organizations, evaluators often have more direct exposure to the operation of controls.

<sup>12</sup> COSO Framework, p. 13.

<sup>13</sup> COSO’s Enterprise Risk Management — Integrated Framework, 2004, includes strategy as an additional objective. The monitoring concepts discussed in this document can be applied equally to monitoring of internal control over strategy.

The interrelationships embodied in the components of the COSO Framework have also been illustrated in the process-oriented graphic included in COSO's 2006 *Internal Control Over Financial Reporting — Guidance for Smaller Public Companies* (COSO's 2006 Guidance). This graphic (modified in Figure 2) depicts the internal control system as a process, whereby the monitoring component evaluates the effectiveness of all five components.



The COSO Monitoring Process  
**Figure 2**

This process view of the COSO Framework shows that internal controls<sup>14</sup> are developed (1) in response to one or more identified risks that affect the achievement of organizational objectives, (2) within the context of an effective control environment, and (3) with proper information and communication. The process includes:

1. Setting objectives;
2. Identifying risks to achieving those objectives;
3. Prioritizing those risks;
4. Designing and implementing appropriate responses to the risks (e.g., internal control);
5. Identifying and prioritizing monitoring needs based on the level of risk, the nature of the controls designed, and the possibility of control failure;
6. Designing appropriate monitoring procedures that use appropriately persuasive information; and
7. Communicating results to management and others and taking any necessary corrective action.

<sup>14</sup> Throughout this discussion document, the terms "internal controls" and "controls" are used to refer to the processes and elements put in place to achieve the objective of any of the five COSO Framework components. The term "control activities," on the other hand, refers specifically to internal controls put in place to achieve the objective of the COSO Framework's control activities component.

Monitoring procedures, when designed and applied effectively, result in action to identify control weaknesses, report them, assess them, and correct their root causes — not just in the control activities component, but throughout the internal control system. Root causes of control weaknesses relate either to the failure of controls to operate as designed due to unintentional or intentional errors (in which case training, discipline, or control redesign may be in order) or to the improper design of controls so as to address the risk effectively (in which case the corrective action involves implementing better controls).

### Difference Between Monitoring Activities and Control Activities

Some monitoring activities may also serve as control activities (and vice versa). To the extent that an activity or process is designed to lead to the timely identification and correction of the root cause of control weaknesses, it is a *monitoring activity*. To the extent that an activity or process leads only to the timely detection and correction of errors, it is a *control activity*. For example, a review of an exception report is a control activity when performed only for the purpose of identifying and correcting those exceptions that are identified as errors. That same review could be a monitoring activity if it is designed to further identify the root cause of possible control weaknesses that caused the errors and to facilitate changes in controls to prevent subsequent control failures.

## II. Fundamentals of Monitoring

The COSO Framework makes clear that monitoring is an assessment by appropriate personnel of the design and operation of controls on a suitably timely basis and the taking of necessary actions. The result of that assessment may or may not be made public through a written report or assertion. COSO’s 2006 Guidance<sup>15</sup> articulated 20 principles — focused on financial reporting<sup>16</sup> — that organizations can use in evaluating whether they are achieving the financial reporting objectives in all five COSO components (see Appendix A).

**COSO’s 2006 Guidance**

“Each of the five components of internal control set forth in the [COSO] Framework is important to achieving the objective of reliable financial reporting. ... When the five components are present and functioning, to the extent that management has reasonable assurance that financial statements are being prepared reliably, internal control can be deemed effective.”

<sup>15</sup> This discussion document is consistent with both the 1992 COSO Framework and COSO’s 2006 Guidance, and it seeks to build on the foundation of good internal control that has been established in both documents.

<sup>16</sup> Although this discussion document is designed to apply to all objectives and components within the COSO Framework, it will concentrate on the financial reporting objective and, thus, on internal control over financial reporting (ICFR). Accordingly, the narrative and examples focus specifically on monitoring ICFR, but clearly parallel the operations and compliance objectives of the COSO Framework.

Although COSO's 2006 Guidance was developed specifically for smaller public companies, the 20 principles can be applied to any organization — large or small, public or private, for-profit or not-for-profit, or governmental — and are not limited to use in year-end evaluations.

#### 1992 COSO Framework

"Monitoring can be done in two ways: through ongoing activities or separate evaluations. Internal control systems usually will be structured to monitor themselves on an ongoing basis to some degree. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. ... Usually, some combination of ongoing monitoring and separate evaluations will ensure that the internal control system maintains its effectiveness over time."

Two of the principles in COSO's 2006 Guidance relate directly to the monitoring component as follows:

Principle 19: "Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time."<sup>17</sup>

Principle 20: "Internal control weaknesses are identified and communicated in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate."<sup>18</sup>

COSO's 2006 Guidance also identified specific attributes that are associated with each principle. These attributes are designed to assist the organization in evaluating whether an approach to monitoring is likely to be effective.

### Attributes of Ongoing Monitoring and Separate Evaluations

Effective monitoring:

- Is integrated, to the extent possible, with operations — Ongoing monitoring is built into the organization's normal operating activities and automated monitoring routines.
- Provides objective assessments — Ongoing monitoring and/or separate evaluations should provide an appropriately objective consideration of internal control effectiveness.
- Uses knowledgeable personnel — Evaluators understand the components being evaluated and how those components relate to the organization's objectives.
- Considers feedback — Management and the board receive feedback on the effectiveness of internal control.
- Adjusts scope and frequency — Management varies the scope and frequency of separate evaluations depending on (1) the importance of underlying controls in

<sup>17</sup> COSO's 2006 Guidance, Principle 19 (see Appendix A).

<sup>18</sup> Ibid., Principle 20.

mitigating meaningful risks to the organization's objectives, and (2) the results of other monitoring procedures.

### **Attributes of Effective Communication and Follow-Up**

No system can provide absolute assurance that control failures will not occur, but an effective system should be designed to identify and correct problems before they become material to the organization's objectives. Principle 20 ("Reporting Deficiencies") from COSO's 2006 Guidance identified three attributes that are consistent with that goal:

- Report findings — Findings of internal control weaknesses are reported (1) to the individual who owns the process and related controls and who is in a position to take corrective actions and (2) to at least one level of management above the process owner.
- Report weaknesses — Significant weaknesses are communicated to top management and the board or audit committee.
- Correct problems on a timely basis — Weaknesses reported from both internal and external sources are considered, and timely corrective actions are taken.

These attributes reinforce the need for the right people to receive information such that (1) corrective action can be taken and (2) management can provide sufficient oversight to gain an understanding that the corrective action has been taken.

### **Elements of Effective Monitoring**

Management implements effective monitoring by (see Figure 3):

1. Establishing an effective control environment for monitoring, including:
  - A tone at the top that stresses the importance of monitoring, and
  - An effective organizational structure that places people with appropriate skills and authority in monitoring roles (see "Capabilities and Position of Evaluators" in Section IV).
2. Prioritizing monitoring procedures based on the importance of controls in managing or mitigating risk (see "Prioritizing and Designing Monitoring Procedures" in Section IV).
3. Establishing a communication structure where:
  - The results of monitoring, including control weaknesses, are reported to the right people in the organization in a timely manner, and

- Prompt corrective actions are taken as necessary (see “Ranking Issues and Reporting Internally” in Section V).



Prerequisites for Effective Monitoring

**Figure 3**

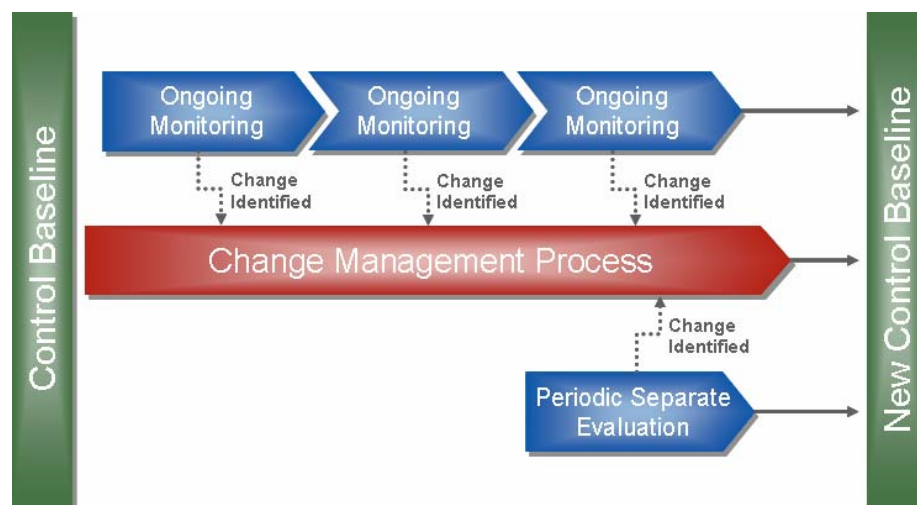
The second element — prioritizing monitoring procedures based on control importance — is often the key to designing effective monitoring programs that are as efficient as possible. Section IV, “Designing Effective Monitoring” discusses prioritization in more detail. At a high level, organizations can build efficient monitoring through a structure that includes the following (see Figure 4):

1. A Control Baseline —Monitoring starts with a supported belief that the internal control system is designed and operating effectively. To the extent that an organization does not already have such a baseline in a given area, it may find it necessary to perform an initial, and perhaps extensive, evaluation of the design and operation of internal control. This control baseline establishes a suitable starting point for more-effective and more-efficient monitoring in the future.
2. A Change-Identification Process — Internal controls change from their baseline for one of two reasons. Either the underlying processes or risks change due to internal or external factors, leading to a necessary change in the *design* of internal controls, or the *operation* of the existing controls changed. In either case, these changes, if not properly managed, are the catalyst for internal control failures. The risk assessment component<sup>19</sup> of internal control is designed to identify changes in processes or risks and verify that the design of underlying controls remains effective. Monitoring evaluates the risk assessment component’s ability to identify those changes. Monitoring also identifies indicators of change in the design or operation of controls and verifies that they continue to meet their objective of helping to manage or mitigate related risks. Such

<sup>19</sup> Chapter 3 of the 1992 COSO Framework discusses the risk assessment component. On p. 44 it states, “Fundamental to risk assessment is a process to identify changed conditions and take action as necessary.”

indicators might include intentional changes in the design of controls or indicators that come from the organization’s ongoing monitoring or separate evaluation procedures.

3. A Change-Management Process — When changes in controls occur or need to occur, effective monitoring verifies that the internal control system manages the changes appropriately and establishes a new control baseline for the changed controls.
4. Control Reconfirmation — When ongoing monitoring procedures only partially support conclusions regarding control performance,<sup>20</sup> effective monitoring periodically reconfirms control operation through separate evaluations using appropriately persuasive information.<sup>21</sup>



Elements of Effective Monitoring  
**Figure 4**

All four components of this structure contribute to the effectiveness of an organization’s monitoring program. The second and third components warrant special attention because they contribute further to the efficiency of monitoring activities and, thereby, to the efficiency of the entire control structure. Effective change-identification and change-management processes provide important information to evaluators that influences their assessment of the risk that controls will fail to manage or mitigate risk — information about changes that *should* be made in controls because the underlying processes or risks change, and information about changes in controls that *have already* taken place, such as changes in personnel performing controls. As a

<sup>20</sup> Ongoing monitoring procedures may only partially support conclusions regarding control performance if the information used does not provide persuasive (i.e., sufficient and suitable) evidence that controls are operating (see “Types of Information Used in Monitoring”). Although such monitoring procedures may not be adequate over the long term to conclude that the underlying controls are effective, they are useful in that they reduce the risk of undetected control failure between separate evaluations.

<sup>21</sup> See the “Nature of Information Used in Monitoring” section for a description of persuasive information.

result, change-identification and change-management processes can influence the scope of other monitoring procedures that may be more costly.

For example, a supervisor responsible for multiple order-entry personnel might increase the scope of monitoring certain controls if the organization adds a new sales channel with different order-entry procedures (i.e., the process changed, possibly impacting the design or operation of controls). He or she might also increase the scope of monitoring if new order-entry personnel are hired (i.e., the change increases the risk that controls will fail due to the inexperience of the personnel). The effective change-identification and change-management procedures can draw attention to areas of heightened risk due to change, allowing the supervisor to vary the type, timing and extent of reconfirmation procedures — thereby improving overall monitoring efficiency. In any case, the supervisor would periodically reconfirm that important order-entry controls are operating correctly.

When change-identification and change-management processes are absent, evaluators have a more difficult time knowing whether the design of controls in place continues to achieve the underlying **control objective**, or whether any factors surrounding the control might indicate that a change in its operation has taken place. The difficulty in identifying and managing such changes can increase the need to perform more-frequent monitoring through separate evaluations using direct information.

### **Role of the Board/Audit Committee**

Controls performed below the senior-management level can be monitored by management personnel or their objective designees. However, controls performed directly by senior management, and controls designed to prevent or detect senior-management override of other controls, cannot be monitored objectively by senior management or its direct reports. In these limited circumstances, monitoring should be performed by the board — often through the audit committee — and its resources (e.g., internal audit).

The board is also in the best position to evaluate whether management has implemented effective monitoring procedures elsewhere in the organization. It makes this assessment by gaining an understanding of how senior management has met its responsibilities.

In most organizations, it is neither feasible nor necessary for the board to understand all of the details of every monitoring procedure, but the board should have a reasonable basis for concluding that management has implemented an effective monitoring system. Boards obtain persuasive information in support of their conclusions through inquiry, observation and oversight of management; the internal audit function (if present); hired specialists (when necessary); and external auditors. They might also consider the output from ratings agencies and financial analysts. Finally, in some circumstances, boards might make inquiries of non-management personnel, customers, and/or vendors.

The board's consideration of the external auditor's results is an important issue. Auditors must maintain their objectivity in both fact and appearance, and, as such, they are not part of an audit client's internal control system. However, an organization that does not appropriately consider the results of the external auditor's work would have a weakness in its monitoring procedures.

If the external auditor's work identifies possible errors or control weaknesses, the organization should consider those results in the context of its own monitoring (i.e., identifying the root cause of the errors or control weaknesses, prioritizing any control weaknesses based on severity, and reporting the results to people who are in a position to take any necessary corrective action). However, neither management nor the board should plan to reduce its monitoring efforts in other areas simply because the auditor did not find errors or control weaknesses.

### III. Nature of Information Used in Monitoring

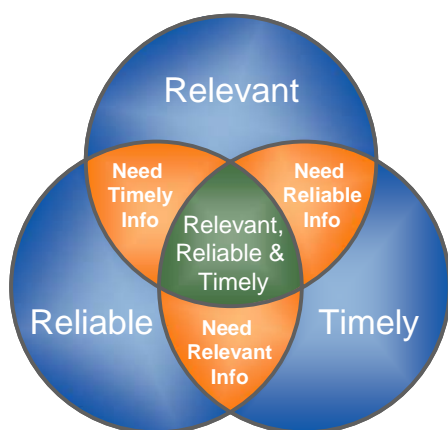
Monitoring involves gathering and analyzing **persuasive information** to support conclusions about the effectiveness of controls within all five COSO components. The **persuasiveness of information** refers to the degree to which the information is capable of providing adequate support for conclusions regarding the effectiveness of controls. Persuasive information is both **suitable** and **sufficient**.

Suitability is a measure of the *quality* of the information in the context for which it is being used, without considering its quantity. It refers to the information's **relevance**, **reliability**, and **timeliness**. Sufficiency is a measure of the *quantity* of information. Suitable information is persuasive if gathered and analyzed in sufficient quantities. Information that is not suitable (i.e., not relevant, reliable, and timely) cannot be sufficient regardless of quantity and, therefore, cannot be persuasive on its own.

Persuasive information gives the evaluator reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of individual controls or a control component. It does so within the constraints of an appropriate cost-benefit analysis that weighs the effort to gather and evaluate monitoring information against the contribution of such information to achieving stakeholder internal control objectives. This analysis is normally qualitative in nature and requires the exercise of appropriate judgment by those responsible for monitoring.

## Information Suitability

Suitable information is **relevant**, **reliable**, and **timely**. Figure 5 demonstrates how these three elements of suitability operate together. In the center of the diagram where the



Elements of Suitable Information  
**Figure 5**

information is relevant, reliable, *and* timely, the evaluator can turn his or her attention to whether enough of the information is available to form a reasonable conclusion.

Information that does not adequately demonstrate all three elements may be suitable to a degree, but alone it cannot support reasonable conclusions regarding continued control effectiveness. For example, information may be relevant and reliable, yet not timely enough to support a conclusion regarding control effectiveness for the period of time under consideration. Alternatively, information may be both relevant and timely, but generated from a less-than-reliable source. Finally, information may be both

timely and reliable, but not adequately relevant to a conclusion about the effectiveness of the related controls. As Figure 5 indicates, in these situations, supplemental information would be required to achieve the required degree of suitability.

### *Relevance of Information*

Information is relevant when it tells the evaluator something meaningful about the operation of the underlying controls or control component. For example, reviewing résumés and training records can tell an evaluator something about whether an accountant has the appropriate background to handle certain areas of complex accounting — the résumés and training records are relevant to controls regarding the financial competence of personnel.

Information that directly confirms the operation of controls is most relevant. Continuing the above example, having firsthand knowledge that an accountant accurately analyzes complex accounting and makes informed choices is more relevant than simply reviewing résumés.

Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information. The following describes the nature and value of direct and indirect information as applied to monitoring.

**Direct information** clearly substantiates the operation of controls. It is obtained by observing controls in operation,<sup>22</sup> reperforming them, or otherwise directly testing their operation. Generally, direct information is highly relevant because it provides an unobstructed view of control operation. Such information can be derived through ongoing monitoring or separate evaluations.

**Direct information is obtained by observing controls in operation, reperforming them, or otherwise directly testing their operation.**

The following are examples of *ongoing monitoring activities* that use direct information regarding controls:

(1) appropriately detailed supervisory reviews of reconciliations upon their completion; (2) routine, objective reviews of system-access-rights reports, confirming that new access rights were granted properly by authorized personnel; or (3) the chief legal officer’s review of background checks on all management new hires, confirming human resources’ proper review and consideration of background information.

Examples of *separate evaluations* that use direct information include: (1) periodic internal audit evaluation of sampled reconciliations; (2) an annual review of access rights to critical systems; (3) internal audit’s annual review of manual journal entry approvals; and (4) periodic audit committee review of background information on selected new hires in key management positions.

**Indirect information** is all other information used to assess whether controls or control components continue to operate effectively, such as data that either relates to or is produced by the process in which the controls reside. Examples of indirect information include, but are not limited to (1) operating statistics, (2) **key risk indicators**, (3) **key performance indicators**, or, possibly, (4) comparative industry metrics.

Indirect information is used to identify anomalies that indicate that a control, or set of controls, may have failed to operate effectively. The absence of such anomalies, however, does not demonstrate explicitly to evaluators that underlying controls are operating effectively. Rather, monitoring using indirect information can provide additional support for conclusions reached through other monitoring procedures and through management’s monitoring of changes in

---

<sup>22</sup> Observing controls in operation is an important monitoring tool when applied properly. In fact, observation may be the only available method of evaluation in situations where a control does not result in some form of documentation that can be evaluated after the fact. For example, a weekly management meeting where past-due receivables are discussed may be an important control in forming proper judgments about receivable collectibility and necessary reserve amounts. An evaluator might determine that observing these meetings is the best way to form reasonable conclusions about the effectiveness of the control. However, observation has limits, especially when the people performing the control know they are being observed. Thus, reperforming or directly testing a control (possibly in combination with observation) may be a more effective monitoring procedure.

systems and processes, as described previously. Thus, through effective monitoring using indirect information, the period of time between separate evaluations may be extended.

**Indirect information is used to identify anomalies that indicate that a control, or set of controls, may have failed to operate effectively. The absence of such anomalies, however, does not demonstrate explicitly to evaluators that underlying controls are operating effectively.**

Assume, for example, that a supervisor must determine whether controls over billing continue to operate effectively. Through a routine review of credit memos, the supervisor finds that no credit memos related to billing errors have been issued for a lengthy period. By itself, a review of credit memos that is free of anomalies does not reveal whether the controls continue to operate effectively — underlying controls may be ineffective, but related problems may not have led (at least yet) to the issuance of credit memos. However, in the presence of an effective monitoring structure (e.g., a baseline of effective billing controls and procedures to identify and manage changes in the billing area), the use of

indirect information can influence the supervisor's decisions about the scope of monitoring regarding billing controls. By gathering and evaluating persuasive information supporting a conclusion that changes have not occurred or are not required, *and* through evaluating indirect information that yields no anomalies, the supervisor may justify performing less-frequent separate evaluations using direct information. Conversely, if changes and/or anomalies are identified, the supervisor may decide to perform more-frequent separate evaluations using direct information.

The value of indirect information in monitoring is proportionate to the strength of the internal control system. For example, indirect information is best able to identify anomalies when the related processes are stable or, at least, when the effects of changes are factored into the analysis. Indirect information is most useful in organizations where the risk assessment process properly identifies and considers any changes in people, processes or technology that might impact control operation or the results of the indirect information. Likewise, indirect information is valuable only to the extent that it is produced accurately and on a timely basis by an effective information and communication structure.

The value of indirect information is *inversely* proportionate to the length of time since the last control baseline was established. As the length of time increases, the ability of the indirect information to flag anomalies decreases, as does the ability to support a conclusion on the continuing operation of controls. The value of indirect information is also inversely proportionate to the significance of underlying risk.

Following is another example of how indirect information might be used. Assume that a manager in a small organization is intimately involved in closing orders and has a clear

perception of total shipments over a period of time (e.g., a week or month). This manager might review sales figures for a time period and have a reasonable basis to conclude whether sales have been billed in a timely fashion and recorded correctly. He or she might then conclude that the risk of control failure regarding timely and accurate billing is reduced to an acceptable level. The manager might also supplement that information with a walk around the plant floor, comparing inventory levels with planned levels, to lend additional support to his or her belief that sales figures are correct.

The manager in this example has concluded that the risk of control failure is reduced to an acceptable level, but he or she has not directly observed or evaluated the controls since the baseline of effective controls was last established. The manager is basing this assessment not only on the persuasiveness of the indirect information above, but also on the persuasiveness of other information gathered and analyzed regarding the internal control system. An organization's ability to use indirect information effectively in this manner depends on the effectiveness of the overall monitoring structure discussed earlier (see "Elements of Effective Monitoring" in Section II).

### *Reliability of Information*

Those responsible for monitoring need a reasonable basis for concluding that the information they are using is reliable. Reliable information is **accurate, verifiable** and comes from an **objective** source. Having accurate information is prerequisite to reaching correct conclusions. Verifiable information enables evaluators to know whether the information can be trusted.

Although accuracy and verifiability are commonly understood, the concept of objectivity warrants further discussion. Objectivity is the absence of bias in the information and relates both to the way in which information is generated and to the characteristics of the individual performing the evaluation of the information. The objectivity of the source of information is the degree to which that source can be expected to provide unbiased data for evaluation. In addition, the individual performing the control evaluation using that data must also be objective in attitude. An objective individual performs the evaluation with no concern about possible personal consequences and no vested interest in manipulating the information for personal benefit or self-preservation. Objectivity is affected by factors that might influence any person to report incompletely or inaccurately the information necessary for evaluators to reach an appropriate conclusion. The personal integrity of people providing information is a primary factor in assessing objectivity, but it is not the only factor. Other factors include compensation incentives, reporting responsibilities, personal relationships, and the degree to which individuals might be affected by the results of monitoring.

### *Timeliness of Information*

To be persuasive, information must be produced and used in a time frame that makes it possible to prevent or detect and correct control weaknesses *before* they become significant to the organization. For example, a single risk might be so important to an organization that even a single failure would have a significant impact on the organization's objectives. In such a case, the organization might decide to monitor controls over that risk through ongoing monitoring of real-time direct information. Another risk might take years of failure to have a significant impact on the organization's objectives. In this case, the organization might monitor the risk by performing either a periodic separate evaluation or a combination of ongoing monitoring and separate evaluations of the underlying controls.

The interval between separate evaluations is based on organizational judgment regarding what constitutes a "reasonable period of time" — with "reasonable" being measured in terms of the ability to prevent or detect and correct a control weakness before it becomes a significant problem. An organization's judgment is influenced by the level of risk, the nature of the control, the frequency of its operation, and the persuasiveness of any ongoing monitoring procedures.

### **Information Sufficiency**

Evaluators must gather *sufficient*, or enough, suitable information to support a reasonable conclusion about control effectiveness. When evaluating the effectiveness of a particular control, sufficiency can refer to the number of instances of that control selected for evaluation (e.g., selecting 30 out of a population of 1,000). Sufficiency can also refer to qualitative assessments of adequacy, particularly when monitoring controls that do not lend themselves to sampling, such as infrequently operating control activities or controls within the other four internal control components. In these cases, the determination regarding sufficiency will be based on the organization's judgments, which should be consistent with reasonable professional expectations.

Evaluators can conclude that they have sufficient, suitable information when, based on the evaluation of that information, they can reasonably conclude either that:

1. The risk of a control failure material to the organization's objectives is below the level of reasonable possibility; or
2. The risk of such a control failure is above the level of a reasonable possibility, and thus a control weakness exists.

As the likelihood and significance of underlying risks increase, evaluators may decide to gather and analyze more information supporting conclusions regarding the controls that help manage or mitigate those risks. For instance, an evaluator monitoring reconciliation controls in

a low- or moderate-risk area might decide to evaluate only a few reconciliations on a monthly basis, with a periodic separate evaluation using a larger sample size. Alternatively, in high-risk areas, that same evaluator might monitor every reconciliation control every month.

The frequency of control operation can also influence the amount of information needed to support a reasonable conclusion regarding control operation. For manual controls that operate infrequently (e.g., those that operate annually, quarterly, monthly, or when unique transactions occur), organizations might monitor a higher percentage of the controls depending on the importance of the control in managing or mitigating meaningful risks to the organization's objectives. As the frequency of control operation increases, many organizations employ various statistical-sampling techniques and software to determine sample sizes and to select and evaluate samples.

Likewise, the nature of certain controls may warrant a higher or lower level of monitoring than others. The following table highlights how the nature of controls might impact the amount of information needed.

Nature of the Control	Possible Impact on the Amount of Information
Complex controls	To address the variables in control operation, complex controls may warrant gathering more information than simple controls.
Controls requiring the exercise of significant judgment	Controls requiring significant judgment (as opposed to those requiring little or no judgment) may warrant gathering more information to support a reasonable conclusion that judgment is being applied correctly in all circumstances.
Controls that address the risk of fraud or are subject to management override	When intentional manipulation (versus unintentional failure) of controls is a plausible risk, evaluators might gather more information regarding the effective operation of controls.
Automated controls	Automated controls generally operate consistently. Therefore, a periodic reconfirmation through evaluation of a single instance of automated controls is often an acceptable monitoring threshold. In such situations, management includes in its monitoring procedures the effectiveness of its program testing, program security, and change-control processes.
Manual controls	For manual controls, the quantity of information necessary will vary depending on the frequency of a control's operation.
Controls that operate in areas with a high degree of change in people, processes, or technology versus controls operating in stable areas	Controls that operate in areas with a high degree of change often warrant gathering and analyzing more information than those operating in more-stable environments.
The relative importance of the control in relation to other monitored controls	To the extent that multiple controls operate to achieve a single control objective, the amount of information gathered related to each of those controls may vary depending on the importance of the control. Conversely, to the extent that a single control can serve to detect errors caused by other control failures, its level of importance might increase.

## IV. Designing Effective Monitoring

Designing effective monitoring involves prioritizing and designing the procedures and deciding when and how often to perform those procedures.

### **Prioritizing and Designing Monitoring Procedures**

To develop effective and efficient internal control systems, management identifies and evaluates risks to achieving the organization's objectives. This activity, ordinarily performed in the risk assessment component of the COSO Framework, allows management to respond<sup>23</sup> to risks by designing and implementing appropriate controls.

The scope of monitoring necessary (i.e., its type, timing, and extent) may vary depending on:

- The size and complexity of the organization (see Section VI, “Scalability of Monitoring”),
- The nature of the organization's operations,
- The purpose for which monitoring is being conducted, and
- The relative importance of the underlying controls in meeting the organization's objectives.

#### *Nature of Operations*

The nature of the organization's operations refers to the degree to which those operations involve high-risk activities or are subject to fraud or significant change. When an organization, or a component of an organization, is subject to a high level of change in people, processes, or technology, those changes increase the risk that the internal control system will fail — either through the failure of existing controls to operate as designed, or through the failure of the internal control system to recognize and implement necessary control changes. Thus, the scope of monitoring in these areas may need to be more extensive than in more-stable areas. Likewise, the potential for fraud or the existence of other mission-critical risks increases the scope that is necessary.

#### *Purpose of Monitoring*

Organizations can monitor controls that address control objectives — or a combination of control objectives — related to operations, financial reporting, compliance with laws and

---

<sup>23</sup> COSO's 2006 Guidance, Chapter II, and COSO's 2004 Enterprise Risk Management — Integrated Framework (COSO ERM), Chapters 5–6, provide useful guidance regarding risk assessment and risk response.

regulations, or strategy. Monitoring of controls might also be performed to satisfy the requirements of internal or external stakeholders. The purpose of a particular monitoring activity may influence the type, timing and extent of monitoring necessary to support reasonable conclusions about the effectiveness of controls. For example, monitoring conducted for the purpose of meeting internal operational objectives may differ in scope from monitoring conducted to satisfy investor and regulatory requirements regarding the adequacy of internal control over financial reporting.

### *Relative Importance of Controls*

Some controls can effectively manage or mitigate more than one risk, or can operate with such precision that they would prevent or detect one or more control failures before those failures become significant. If monitoring one or a few controls can adequately address the underlying risk, an organization might include only those controls within the scope of a particular monitoring program. Alternatively, it might design procedures such that some controls are monitored using ongoing monitoring, with periodic separate evaluations of other controls to support the overall conclusions.

For example, assume an organization has a single debt instrument. A risk of misstatement in interest expense may be adequately addressed by the CFO's quarterly comparison of the actual interest-expense rate (i.e., total interest expense divided by the average debt balance) to the interest rate in the debt agreement. Such a comparison is a control activity, and although it does not tell the evaluator with certainty whether controls over calculating and recording interest expense are operating correctly, it does reveal whether interest expense was calculated and recorded correctly during the period. In this example, as long as the interest-expense recalculation control activity continues to operate with an acceptable level of precision, its operation can reduce or eliminate the need to monitor other related controls (i.e., because its effective operation would detect any weaknesses in the controls leading up to the recording of interest expense).

As more variables are added to the operation of control activities, however, their ability to operate at a high level of precision diminishes. Continuing the earlier example, having multiple debt agreements with differing terms would reduce the ability of a simple average-interest-rate calculation to detect a material misstatement before it is published in the financial statements.

Monitoring is most effective and efficient when organizations prioritize and allocate resources where they are needed most. The level of need is based on the importance of controls in managing or mitigating risks to achieving the organization's objectives.

In determining which controls are important, management also considers the expectations of stakeholders. For example, in a financial-reporting context, investor expectations are an essential consideration. Regulatory bodies might also influence which controls are deemed

important. The following table demonstrates how organizations might vary their monitoring approach and the information used in monitoring based on the importance of various controls.

Control Importance	Determining Factors	Possible Monitoring Approach
Highest	Controls addressing risks with high likelihood and high significance	Ongoing monitoring using direct and indirect information, with periodic separate evaluations of direct information
Moderate in short term	Controls addressing risks with low likelihood but high significance	Ongoing monitoring using indirect information, with periodic separate evaluations of direct information
Moderate in long term	Controls addressing risks with high likelihood but low significance	Ongoing monitoring using indirect information, with less-frequent separate evaluations of direct information
Lowest	Controls addressing risks with low likelihood and significance	Might not be monitored at all by senior management or, possibly, may be monitored by relatively infrequent separate evaluations

Ongoing monitoring or separate evaluations using direct information may already be part of normal operations, particularly for high-risk areas on which management and the board focus naturally (e.g., controls over accounting for derivative transactions in some organizations). Management and/or the board may also gather and analyze indirect information for other monitoring purposes. In any case, the organization should consider the persuasiveness of existing monitoring and develop additional procedures only where and if necessary.

#### *Ongoing Monitoring Using Direct Information*

When sufficient direct information is available, ongoing monitoring techniques (e.g., observation, reperformance, or direct evaluation of a control) provide the most persuasive evidence that a control is operating as intended. Because these procedures (1) occur frequently, (2) are integrated with operations, and (3) provide direct information about control operation, they generally have the greatest ability to identify control weaknesses before those weaknesses can significantly affect the organization's objectives. Accordingly, ongoing monitoring using sufficient direct information is especially valuable in areas where the risk is so significant that a few or, possibly, even a single control failure will prevent the organization from achieving its objectives.

*Ongoing Monitoring Using Indirect Information*

Ongoing monitoring using indirect information (e.g., operating statistics, key risk indicators, key performance indicators, and comparative industry metrics) helps support a continued belief that controls continue to operate effectively. As noted earlier, this continued belief is contingent upon the establishment of a reasonably recent control baseline, and the presence of appropriate change-identification and change-management procedures.

As noted earlier, the value of indirect information in monitoring is inversely proportionate to the significance of underlying risk. When the potential impact of a given risk is high, organizations generally perform more-frequent separate evaluations using direct information. When the significance is low (i.e., the organization can afford to miss several or many control failures before they accumulate to the level of materiality), organizations tend to utilize more indirect information, coupled with less-frequent separate evaluations using direct information.

*Separate Evaluations Using Direct or Indirect Information*

Separate evaluations periodically substantiate conclusions about control effectiveness, particularly conclusions arrived at as a result of ongoing monitoring using indirect information. They employ the same techniques as ongoing monitoring, but are performed less frequently, often by people not involved with the operation of the control.

*Capabilities and Position of Evaluators*

In the monitoring process, there are people who are responsible for determining what and how to monitor, assessing the monitoring information, and reaching conclusions regarding the effectiveness of controls. This discussion document refers to such people as “evaluators.” An evaluator may be a single individual in a small organization or, in a large organization, multiple individuals reporting to more-senior evaluators. Regardless, it is important that someone in the organization with appropriate skills, knowledge, and authority understands the risks that the controls are intended to mitigate in order to design and implement appropriate monitoring procedures.

**1992 COSO Framework**

“The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of the internal control system is a matter of management's judgment. ... Usually, some combination of ongoing monitoring and separate evaluations will ensure that the internal control system maintains its effectiveness over time.”

The right side of the COSO Framework cube (see Figure 6) illustrates how internal control systems, including monitoring, might be viewed across an organization. It also demonstrates



The COSO Internal Control  
Integrated Framework  
**Figure 6**

that individuals at every level in an organization may have some monitoring responsibility.

There are people involved in the monitoring process who — although they do not have the responsibility for designing monitoring procedures or for reaching final conclusions regarding control effectiveness — do produce information the evaluators use to reach their final conclusions. For example, a divisional controller may have certain monitoring procedures dictated from the home office, or he or she may provide physical inventory data to a regional manager who will then evaluate the information. These personnel are vital to the

monitoring process because they often provide much of the information used by more-senior evaluators in reaching their conclusions.

**Competence** and **objectivity** considerations help organizations determine who should perform monitoring procedures. Competence refers to the evaluator’s knowledge of the controls and related processes, including how controls should operate and what constitutes a control weakness. As noted earlier, effective monitoring requires both the identification of control weaknesses (if any) and an analysis of the root causes of control failures. Therefore, the evaluator must have knowledge of the underlying control and the risks that the control is designed to mitigate. Maintaining documentation of control activities can be useful in that regard.

Objectivity can be viewed along a continuum from least to most objective (see Figure 7). Self-review<sup>24</sup> is the evaluation of one’s own work, is not objective and, thus, does not constitute monitoring. Instead, it operates as a control activity designed to prevent or detect errors in the normal course of business.

<sup>24</sup> The term “self review” in this document refers narrowly to the review of one’s own work. It should not be confused with the term “self assessment,” which is a broad term that can refer to different types of procedures performed by individuals with *varying degrees of objectivity*. The term “self assessment,” as it is often used, can include assessments made by the personnel who operate the control, as well as other, more-objective personnel who are not responsible for operating the control. In this document those “other, more-objective personnel” would include persons performing peer or supervisory review.



Objectivity in Assessment  
**Figure 7**

Peer review, which is somewhat objective, is the evaluation of a coworker’s or peer’s work. Supervisory review of a subordinate’s work is more objective still. Both peer and supervisory review are valuable — especially when performing ongoing monitoring procedures — because the individuals involved are usually in close proximity to the control and, as a result, are best able to identify and correct control weaknesses promptly.

The most objective form of monitoring is performed by evaluators who are impartial with respect to the operation of the control. Such impartial monitoring often includes evaluations performed by an internal audit function, people from other departments, or external parties. Because impartial evaluators are often distant from the operation of controls, it is sometimes more difficult to employ them in ongoing monitoring using direct information. Accordingly, impartial reviews using direct information usually take the form of separate evaluations. Impartial ongoing monitoring using indirect information often occurs through the review of operating statistics by management personnel or internal audit.

*Using Technology for Effective Monitoring*

Organizations often use information technology (IT) to enhance monitoring through the use of control monitoring tools and process management tools.

Control monitoring tools — Automated control monitoring tools can play a significant role in enhancing the effectiveness, efficiency, and timeliness of monitoring specific controls. Many operate as controls and, simultaneously, provide monitoring information on the continued operations of other controls. Some are implemented independently of the controls they are monitoring, whereas others are part of reporting-capability tools that are otherwise an integral part of the internal control system. Monitoring tools typically focus on one or more of the following:

- Transaction data — Comparing processed transaction (or masterfile) data against a set of control rules to highlight exceptions and/or identify instances in which the controls over a process or system are not working as intended.
- Conditions — Examining application or infrastructure configuration settings/parameters and comparing them with a baseline or with previously established expectations.

- **Changes** — Identifying and reporting changes to critical resources, data, or information, making possible the verification that changes are appropriate and authorized.
- **Processing integrity** — Verifying and monitoring the completeness and accuracy of data as it progresses through various IT processes and systems.
- **Error management** — Monitoring the volume and resolution of activity in suspense areas, typically as part of an application system.

**Process management tools** — Process management tools are designed to make monitoring more efficient and sustainable by automating some monitoring activities, including assessing risks, defining and evaluating controls, and communicating results. These tools are most often used in situations in which responsibilities for controls are distributed throughout multiple or geographically dispersed business units, but they can also be of value to any organization — including smaller ones. Most of these tools use workflow techniques to provide structure and consistency to the performance of monitoring procedures. Some features that make these tools useful include their ability to:

- Coordinate the risk assessment process at both the entity and transaction-flow levels;
- Provide a repository for process, control, and monitoring documentation;
- Enhance the communication process as it relates to the identification, evaluation, and resolution of internal control weaknesses, including their severity and any remediation activities;
- Support the “roll-up” of information about risks and controls at various levels and points within an organization; and
- Provide simplified dashboards showing relevant control performance indicators and the current status of differing aspects of management’s control evaluation process.

All of these tools help a well-controlled organization identify where risks or control operating conditions may have changed. As a result, they provide valuable ongoing monitoring information.

### **Deciding When and How Often to Monitor**

Ongoing monitoring and separate evaluations differ in that ongoing monitoring is ingrained in the daily operations of the organization. As such, it allows the evaluator to identify potential internal control problems on a real-time, or nearly real-time, basis. Ongoing monitoring can occur continuously, especially through the use of automated control monitoring software. It can also be performed on a daily, weekly, monthly, or even annual basis, depending on how often the underlying controls operate. For example, the review of exception-resolution reports for the purpose of verifying that exceptions were properly resolved and root causes were

corrected may cover all identified exceptions, but such a review may occur only once per week. To determine how often ongoing monitoring procedures should be performed, organizations consider the likelihood and significance of the risk's occurrence between evaluations. As the level of risk increases, the interval between monitoring procedures decreases.

As noted in "Elements of Effective Monitoring" in Section II, an organization's change-identification and change-management processes form much of the support for these decisions. To the extent evaluators obtain reasonable support that risks and controls have not changed in a given area since the last control baseline was established, they might perform less-frequent separate evaluations. Where changes have or should occur, effective change-management procedures will establish a new control baseline for future monitoring.

## V. Communicating and Addressing the Results of Monitoring

### **Ranking Issues and Reporting Internally**

Consistent with Principle 20 of COSO's 2006 Guidance, effective monitoring includes identifying control weaknesses and communicating them to the right people in a timely manner. Some organizations accomplish this goal by ranking identified control issues by severity along a continuum such as high, medium, or low, or along a numerical scale (e.g., 1–5 or 1–10). Regardless of the scale used, the two factors that most influence the final ranking are "likelihood" and "significance." In the context of ranking identified control weaknesses, likelihood is the probability that a control will fail to prevent or detect a risk's occurrence, and significance is the potential impact of the risk if it occurs. Section IV, on "Prioritizing and Designing Monitoring Procedures," addressed the effect of likelihood and significance on the prioritization of controls to be monitored, whereas this section calls for a reassessment of these factors given the information learned from the monitoring activities. With a control weakness identified, the organization can gauge the likelihood that controls will fail to prevent or detect the occurrence of a given risk, or whether, collectively, multiple weaknesses affecting the same risk might represent a significant control problem. also In addition, it can better quantify the potential significance of the risk in the event that one or more controls fail to operate properly.

When other compensating controls exist, an individual control weakness may not be assigned a higher ranking. Compensating controls, if operating effectively and monitored, can reduce the severity of an otherwise serious weakness. Accordingly, when determining the severity of control weaknesses, evaluators should consider the impact of all the controls established to address a given risk. In addition, the significance of a potential error related to a control weakness may be low enough that the organization can sustain multiple failures related to the

error. The following table describes how an organization might consider the likelihood and significance variables in the process for prioritizing control weaknesses.

Control Failure		Ranking Considerations
Likelihood	Significance	
High	High	Highest priority – These control weaknesses deserve immediate attention. Additional oversight or review often can be implemented during the correction period to protect further against material errors.
Low	High	Moderate to high priority in the near term – The significance of the potential errors related to these control weaknesses makes them important to correct. Additional oversight or review might also be implemented here during the correction period.
High	Low	Moderate priority in the long term – Potential errors resulting from these weaknesses can accumulate to material levels over time, or they can reduce organizational efficiency as frequent errors must be corrected repeatedly.
Low	Low	Lowest priority – The errors related to these control failures often result more in lost efficiencies than in material errors. Management should consider these for correction, but not at the expense of failing to correct higher-ranking weaknesses.

Reporting protocols vary depending on the purpose for which the monitoring is conducted and on the severity of the weaknesses. Typically, the results of monitoring conducted for purposes of evaluating an organization’s entitywide objectives are reported to senior management and the board. Examples include monitoring of internal control over financial reporting or monitoring of controls over operations that are material to profitability.

However, some monitoring is conducted for purposes that might be material only to a small part of an organization. An example might be operational monitoring conducted in a small subsidiary to meet local goals that are not material to the consolidated company. Identified weaknesses in this case might have “higher likelihood” and “higher significance” relative to the subsidiary’s objectives, but not to the overall organization’s. In such situations, reporting might be limited to local management personnel for whom the local goals are important. In any case, control weaknesses should be reported to the person responsible for the control’s operation and to at least one level higher. Reporting at least to these two levels gives the responsible person the information necessary to correct control operation and also helps ensure that appropriately objective people are involved in the severity assessment.

Regardless, identified control weaknesses, once prioritized, should be corrected within a reasonable time period based on severity. The correction may involve modifying the existing control or implementing other controls. In deciding how to correct weaknesses, organizations compare the cost to correct the weakness, plus any ongoing costs (such as those incurred by implementing an additional control), against the severity of the weakness.

## Reporting to External Parties

Many organizations are required to report to third parties on the effectiveness of their controls. An appropriately designed and executed monitoring program supports external assertions because effective monitoring provides persuasive information that controls operated effectively during the period. However, organizations that are required or plan to report externally on the effectiveness of their controls may design and execute monitoring activities differently than other entities.

### *External Assertions*

The external users of an organization's assertion regarding internal control effectiveness do not have a detailed knowledge of the entity's environment or controls. Users may also be numerous, and the assertion may be used for multiple purposes. Finally, regulations may require more-frequent assertions on control effectiveness than management would perform solely for internal purposes. Evaluators, therefore, may need or desire more persuasive information to support external assertions than they would need to support internal conclusions regarding control effectiveness.

**An appropriately designed and executed monitoring program supports external assertions.**

### *Use of Monitoring Documentation by Others*

When monitoring activities are performed by individuals who are objective, external parties (such as auditors or examiners) are likely to consider the results to be more reliable than those compiled by someone less objective. Organizations have choices regarding the evaluator's level of objectivity and should consider the cost of increasing the objectivity of the monitoring information (e.g., by instituting a peer review or directing internal audit to perform testing) compared with the cost of having the third party, such as an external auditor, develop his or her own reliable evidence. It may be cost-effective to implement a more-objective monitoring process than would otherwise be necessary if the entity did not have an external audit or examination requirement.

Similarly, the decision to use indirect rather than direct information to monitor the effectiveness of controls could involve a cost-benefit evaluation with respect to auditor attestation requirements. For example, an organization's external auditors may determine, based on their audit plan, to test the operation of certain controls. If the organization uses *direct* information in monitoring those controls, the independent auditors might determine to use the results of that monitoring to provide support for their audit conclusions. Conversely, if the organization uses *indirect* information in monitoring the controls, the independent auditors

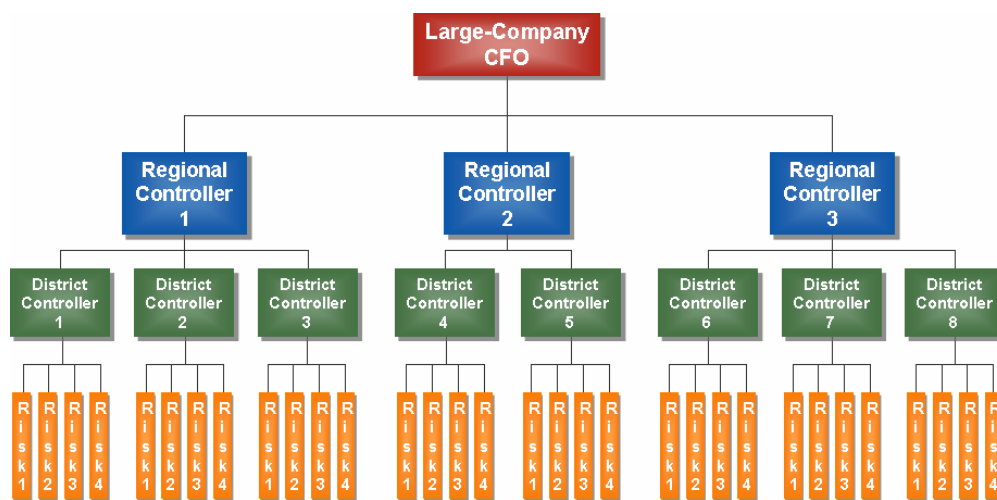
may find it necessary to perform their own separate tests of direct information — possibly increasing the cost of the audit. Thus, when designing its monitoring procedures, the organization might consider the overall costs involved in both monitoring and the independent audit.

## VI. Scalability of Monitoring

Many factors can influence the type, timing, and extent of monitoring in an organization. Two factors that warrant special mention are organizational size and complexity.

### Scalability Based on Size

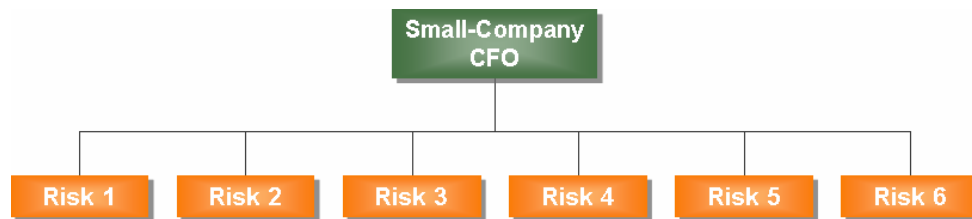
Organizational size affects the design and conduct of monitoring. In most large organizations neither senior management nor the board are in close proximity to the operation of many controls. As a result, they must rely more on other competent and objective parties to perform procedures on their behalf. Most often, monitoring procedures in large organizations are conducted by successive levels of management. These procedures are built in to the day-to-day, ongoing monitoring activities that operate at each level of the organization (Figure 8), all of which “roll up” to a home office or headquarters, and are typically augmented by separate



Sample Large-Company Monitoring Structure  
**Figure 8**

evaluations performed by a qualified internal audit function or other parties (e.g., lower-level management or other departments). These periodic separate evaluations lend support to the conclusion that the smaller monitoring systems are operating effectively.

On the other hand, monitoring at the senior-management level in smaller organizations often occurs much closer to the risk and related controls, giving the evaluators more implicit knowledge of the operation of controls. Monitoring in the smaller organization (Figure 9) can look much like monitoring at lower levels in a large organization (Figure 8). The primary difference is that the lead evaluator (the CFO in the examples) in the larger organization performs more monitoring of other monitoring procedures, whereas the lead evaluator in the smaller organization performs more monitoring of actual internal controls.



Sample Small-Company Monitoring Structure

**Figure 9**

Large companies do have the advantage of scale. Because their risks are more dispersed, control problems in only one area may not be significant. For example, a company that has 20 people processing invoices, one of whom is not properly trained, may be able to operate for some time without material error. On the other hand, a company that has only one person processing invoices cannot afford for that person to be improperly trained — such a weakness would increase the significance of management’s daily observation of critical internal controls. In addition, management’s objectivity in a smaller organization may be impaired by the fact that it performs some of the control activities that are subject to monitoring, thereby increasing the importance of monitoring performed by the board or audit committee.

**Scalability Based on Complexity**

Size notwithstanding, some organizations are more complex than others. Factors influencing complexity include industry characteristics, regulatory requirements, number of products or service lines, level of centralization versus decentralization, use of prepackaged versus customized software, or the presence of complex transactions (e.g., complex capital structures, derivative transactions, or acquisitions).

Because the level of complexity may vary by department or area, scaling of monitoring based on complexity is more difficult to apply to an entire organization than is scaling based on size. An organization may use a prepackaged information system, reducing IT risk, but that same organization might enter into derivative contracts, increasing accounting risk.

Level of complexity generally correlates with level of risk. Accordingly, in areas of greater organizational complexity, one would expect more-intense monitoring using direct information. In contrast, in areas of less complexity, ongoing monitoring using indirect information would be appropriate, along with periodic confirmation through separate evaluations that use direct information.

### **Formality of Monitoring and Level of Documentation**

As organizations increase in size and complexity, they may find an increased need for formality in their monitoring activities. This need becomes increasingly important when external reporting requirements exist. The increased formality may include areas such as:

- Automated and manual processes to document and retain monitoring information.
- Detailed policies and processes regarding aggregation, evaluation, and reporting of weaknesses to senior management and the audit committee.

Such increased formality can improve the efficiency and effectiveness of monitoring in a large or complex organization. It may also improve the efficiency and effectiveness of external parties, such as auditors or examiners, who might separately evaluate internal control.

Absent an external reporting requirement, smaller organizations may require less documentation to support conclusions regarding control effectiveness — especially where senior management and the board have implicit knowledge of control activities. As organizations increase in size, the level of implicit knowledge decreases at the senior-management and board levels, thus increasing the need for monitoring documentation. Likewise, when external assertions are required, organizations should maintain documentation of the monitoring activities and results in support of the organization's conclusions about control effectiveness.

## **VII. Conclusion**

Effective internal control systems enable organizations to manage risks and uncertainties in their environment and processes and in the information they use to make decisions. They promote efficiency, reduce risk of loss, and help ensure the reliability of financial statements and compliance with laws and regulations. Effective internal control systems are built into the activities of an organization's people and into its policies, procedures and technology. The five components of an internal control system — control environment, risk assessment, control activities, information and communication, and monitoring — all work in concert to provide the organization with reasonable assurance that it can realize its objectives.

If the control environment is the foundation of an effective system of internal control, then monitoring is the capstone. Monitoring serves two primary purposes. First, it provides

management and the board with information that helps them conclude that the internal control system is working as intended over time. Second, it promotes good control operation because personnel responsible for the controls being monitored know that proper control operation is verified. The adage is true — “You get what you *inspect*, not what you *expect*.”

This discussion document is intended to reinforce and clarify, not add to, the sound principles of monitoring previously established through the 1992 COSO Framework and COSO’s 2006 Guidance. Its goal is to help organizations develop monitoring programs that will contribute most effectively and efficiently to the operation of an optimal internal control system.

The monitoring process as described above and in this discussion document is not intended to be a “cookbook” for how to monitor. Rather, it is designed to help organizations take a holistic view of monitoring, recognize elements critical to effectiveness, and identify specific points in their own monitoring where weaknesses might be mitigated or eliminated.

Managing risks to organizational objectives, while allowing for the proper pursuit of opportunities, is the ultimate goal of every effective internal control system. Monitoring is a cost-effective approach to providing timely information about the continued effectiveness of an internal control system. As such, effective monitoring should be a net benefit to organizations and their stakeholders.



## Principles of Effective Internal Control Over Financial Reporting

COSO's 2006 publication, *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, provides a set of 20 basic principles representing the fundamental concepts associated with, and drawn directly from, the five components of the framework. These principles are listed below, organized by COSO component.

### Control Environment

1. Integrity and Ethical Values — Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
2. 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. 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 policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

### Risk Assessment

8. Financial Reporting Objectives — Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.
9. 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. Fraud Risk — The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

## **Control Activities**

11. **Integration with Risk Assessment** — Actions are taken to address risks to the achievement of financial reporting objectives.
12. **Selection and Development of Control Activities** — Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
13. **Policies and Procedures** — Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.
14. **Information Technology** — Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

## **Information and Communication**

15. **Financial Reporting Information** — Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and time frame that supports the achievement of financial reporting objectives.
16. **Internal Control Information** — Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and time frame that enables personnel to carry out their internal control responsibilities.
17. **Internal Communication** — Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.
18. **External Communication** — Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

## **Monitoring**

19. **Ongoing Monitoring and Separate Evaluations** — Ongoing monitoring and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.
20. **Reporting Weaknesses** — Internal control weaknesses are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

## Glossary

Accuracy	The degree to which information can reasonably be expected to be free from error and/or to communicate results that reflect reality.
Board monitoring	Board monitoring is the execution of monitoring procedures by the board, its committees, or others charged with overseeing management conduct. It involves monitoring management performance in relation to all of the COSO components, including monitoring management's own monitoring process. It also includes monitoring those controls that management cannot monitor objectively, such as monitoring controls performed directly by management and monitoring the risk of management override.
Competence	Competence refers to the evaluator's knowledge of the controls and related processes, including how controls should operate and what constitutes a control weakness.
Control activities	Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achieving objectives. Control activities occur throughout the organization, at all levels, and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
Control baseline	A control baseline is a point in time at which an organization has persuasive information supporting a reasonable conclusion that controls across the entire organization, or in a given area, are effective. A control baseline serves as a suitable starting point for effective control monitoring.
Control environment	The control environment sets the tone of an organization by influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include: <ul style="list-style-type: none"><li>• The integrity, ethical values, and competence of the entity's people;</li><li>• Management's philosophy and operating style;</li><li>• The way in which management assigns authority and responsibility, and in which it organizes and develops its people; and</li><li>• The attention and direction provided by the board of directors.</li></ul>

Control objectives	Control objectives provide specific targets against which to evaluate the effectiveness of controls. Typically they are stated in terms that describe the nature of the risk they are designed to help manage or mitigate. For example, a control objective that all transactions should be properly authorized relates to the risk that improper, unauthorized transactions will occur.
Direct information	Direct information is information that directly substantiates the operation of controls and is obtained by observing them in operation, reperforming them, or otherwise directly evaluating their operation. Direct information is generally highly persuasive because it provides an unobstructed view of control operation. It can be obtained from either ongoing or separate evaluations, but it must link directly to a judgment regarding the controls.
Evaluator	Evaluators are individuals within the organization who have appropriate skills, knowledge, and authority and who also understand the risks that the controls are intended to mitigate. They require this understanding in order to ensure that appropriate monitoring procedures are designed and implemented. The two primary attributes of effective evaluators are competence and objectivity.
Indirect information	Indirect information is information (other than direct information) that is relevant to assessing whether an underlying risk is mitigated and controls are operating. Indirect information does not tell the evaluator explicitly that underlying controls are operating effectively, but in the presence of an effective monitoring structure (including a control baseline, change-identification/management procedures, and periodic control reconfirmation), persuasive indirect information can influence the type, timing and extent of monitoring procedures using more-direct information.

Information and communication	Information and communication refer to the nerve-center function of an internal control system. Pertinent information — internal and external — must be identified, captured, and communicated in a form and time frame that enable personnel to carry out their responsibilities. Information systems use or produce reports containing operational, financial, and compliance-related information, all of which make it possible to operate and control the business. Effective communication must also occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.
Internal control	Internal control is a process effected by an entity’s board of directors, management, and other personnel, and it is designed to provide reasonable assurance that organizational objectives can be met.
Key performance indicators	Key performance indicators are metrics that reflect critical success factors. They help organizations measure progress towards goals and objectives.
Key risk indicators	Key risk indicators are forward-looking metrics that seek to identify potential problems, thus enabling an organization to take timely action, if necessary.
Material or materiality	Materiality is a fundamental concept that helps distinguish the important from the trivial in a specific discipline or application. It furnishes a threshold determination of criticality, and, with respect to exercising judgment, permits a decision-maker to omit from consideration issues that do not matter (cf. Ernest L. Hicks, 1964, <i>Journal of Accounting Research</i> ). In a financial reporting context, an error is material if it would be reasonable to conclude that a user of financial statements would alter his or her decisions as a result of the identified intentional or unintentional error.

Objective or objectivity	Objectivity is a measure of the factors that might influence any person to report inaccurately or incompletely information necessary for evaluators to reach appropriate conclusions. It includes personal integrity, as well as factors that might motivate even a person with perceived high integrity to misrepresent facts, such as having a vested, personal interest in the outcome of the monitoring procedures.
Ongoing monitoring	Ongoing monitoring relates to activities that serve to monitor the effectiveness of internal control in the ordinary course of operations, including regular management and supervisory activities, comparisons, reconciliations, and other routine actions.
Persuasiveness of information or persuasive information	The persuasiveness of information refers to the degree to which the information provides support for conclusions. The level of persuasiveness is derived from its suitability (i.e., its relevance, reliability, and timeliness) and its sufficiency.
Reasonable assurance	The definition of “reasonable assurance” varies depending on the context in which it is being used. In the Securities and Exchange Commission’s “Guidance Regarding Management’s Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934” (p. 3), reasonable assurance is defined as the “degree of assurance as would satisfy prudent officials in the conduct of their own affairs.” The American Institute of Certified Public Accountants (AICPA) defines reasonable assurance for auditors as “a high, but not absolute, level of assurance.” (See AICPA Statements on Auditing Standards (SAS) No. 1, Section AU 230, ¶10.) For purposes of this discussion document, the reasonable assurance provided by an effective system of internal control is a level of assurance that is not absolute, but that does provide a person competent in matters related to internal control with a sound basis for concluding whether the organization’s related objectives are likely to be met.
Relevant information	Relevant information tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls (see “Direct information”) is most relevant. Information that relates indirectly to the operation of controls (see “Indirect information”) can also be relevant, but is less relevant than direct information.
Reliable information	Reliable information is accurate (see “Accuracy”), verifiable (see “Verifiable”) and from an objective source (see “Objective”).

Risk assessment	Every entity faces and must assess a variety of risks from external and internal sources. A precondition for risk assessment is establishing objectives that are linked at different levels and internally consistent. Risk assessment is the identification and analysis of risks relevant to realizing objectives, and it serves as a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, flexible mechanisms are needed to identify and address the special risks associated with change.
Separate evaluations	Separate evaluations seek to draw inference about the consistent operation of controls by evaluating controls at a specific point or over a specific period of time. Separate evaluations can make use of all of the techniques used in ongoing monitoring, but they are employed less frequently and are often based on a sample of instances in which the controls operate.
Sufficient information	Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. However, in order for information to be sufficient, it must first be suitable.
Suitable information	Suitable information is relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source), and timely (i.e., produced and used in an appropriate time frame).
Timely information	Timely information is produced and used in a time frame that makes it possible to prevent or detect control weaknesses before they become significant to an organization.
Verifiable or verifiability	Verifiable information is information that can be established, confirmed or substantiated as true or accurate.

