

2010

# COSO Internal control - integrated framework: Guidance on monitoring internal control systems, Volume II: Application

Committee of Sponsoring Organizations of the Treadway Commission

Follow this and additional works at: [https://egrove.olemiss.edu/aicpa\\_assoc](https://egrove.olemiss.edu/aicpa_assoc)

 Part of the [Accounting Commons](#), and the [Taxation Commons](#)

---

**Committee of Sponsoring Organizations of the Treadway Commission**

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

[www.coso.org](http://www.coso.org)

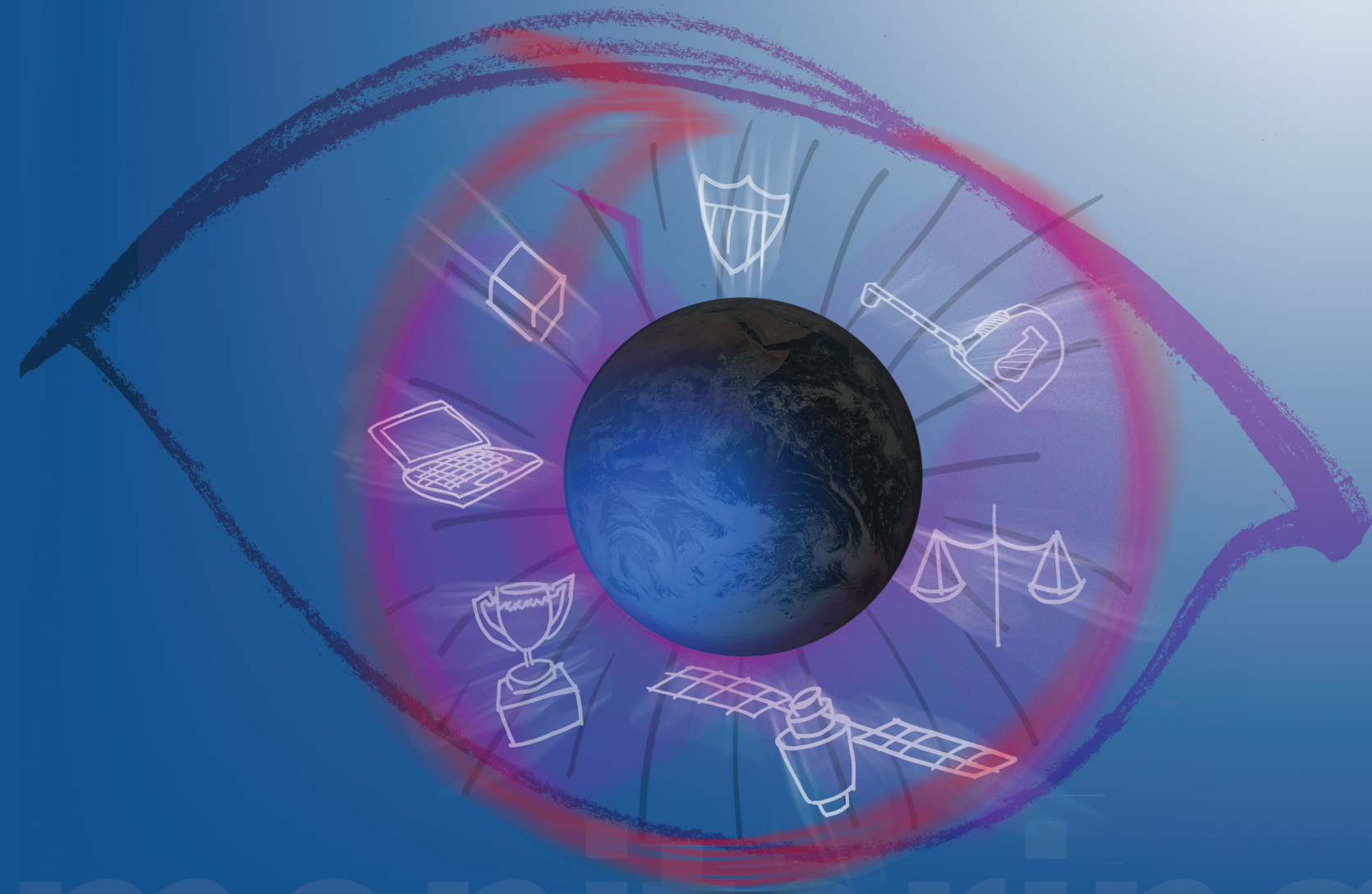


COMMITTEE OF SPONSORING  
ORGANIZATIONS OF THE TREADWAY COMMISSION

# Internal Control — Integrated Framework

## Guidance on Monitoring Internal Control Systems

Volume II : Application



monitoring



# Guidance on Monitoring Internal Control Systems

Volume II: Application

January 2009

Copyright © 2009-2010, The Committee of Sponsoring Organizations of the Treadway Commission (COSO).  
2 3 4 5 6 7 8 9 0 PIP 1 9 8 7 6 5 4 3 2 1 0

*All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions please contact the American Institute of Certified Public Accountants, licensing and permissions agent for COSO copyrighted materials. Direct all inquiries to [copyright@aicpa.org](mailto:copyright@aicpa.org) or to AICPA, Attn: Manager, Rights and Permissions, 220 Leigh Farm Rd., Durham, NC 27707. Telephone inquiries may be directed to 888-777-7707.*

Additional copies of this work may be obtained by visiting [www.cpa2biz.com](http://www.cpa2biz.com).

ISBN 0-87051-795-3



I. Monitoring as a Component of Internal Control Systems	1
Role of Monitoring	2
Structure of Effective Internal Control Systems	4
A Model for Monitoring	7
II. Establish a Foundation for Monitoring	9
Tone at the Top	9
Organizational Structure	10
Baseline Understanding of Internal Control Effectiveness	15
III. Design and Execute Monitoring Procedures	19
Prioritize Risks	21
Identify Key Controls	24
Identify Persuasive Information	29
Implement Monitoring Procedures	40
IV. Assess and Report Results	46
Prioritize and Communicate Results	46
Report Internally	48
Report Externally	49
V. Other Considerations	52
Monitoring Controls Outsourced to Others	52
Using Technology for Monitoring	52
Formality and Level of Documentation	54
Scalability of Monitoring	55
VI. Assessing the Effectiveness and Efficiency of Monitoring	58
Appendix A: Principles of Effective Internal Control Over Financial Reporting	A-1
Appendix B: Map Linking the Model for Monitoring to the 1992 COSO Framework	B-1
Glossary	Glossary-1



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

1. In 1992, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the *Internal Control – Integrated Framework* (the COSO Framework), consisting of five interrelated and equally important components (Figure 1). Four components relate to the design and operation of the system of internal control: control environment, risk assessment, control activities, and information and communication. The fifth component – monitoring – is designed to “ensure that internal control continues to operate effectively.”<sup>1</sup>



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

2. In 2006, COSO published the *Internal Control Over Financial Reporting – Guidance for Smaller Public Companies* (COSO’s 2006 Guidance), which further developed the understanding of how all five internal control components work cohesively to form an effective internal control system. Although targeted to smaller public companies’ reporting on internal control over financial reporting, COSO’s 2006 Guidance contains information that should be (1) helpful to all organizations, regardless of size,<sup>2</sup> and (2) relevant to all of the COSO objectives. Its 20 principles (reproduced in Appendix A) and supporting attributes clarify the COSO Framework so that organizations might apply the Framework more effectively and efficiently. Principles 19 and 20 relate specifically to monitoring – namely, (1) monitoring procedures are designed and implemented to provide information on whether the internal control system operates effectively over time, and (2) internal control **deficiencies**<sup>3</sup> 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>1</sup> COSO Framework, p. 69.

<sup>2</sup> See COSO’s 2006 Guidance, Frequently Asked Questions Volume, Question #17.

<sup>3</sup> See Glossary for definitions of terms set in boldface.



3. The primary factor leading to the development of this guidance was the observation by COSO that many organizations were not effectively utilizing the monitoring component to support conclusions about the effectiveness of internal control over financial reporting. Some organizations had effective monitoring in certain areas, but were not optimizing the results of that monitoring to support their conclusions about the effectiveness of internal control. Instead, they were adding redundant, often unnecessary procedures designed to evaluate controls for which management — through its existing monitoring efforts — already had sufficient support. In other cases, organizations were not making the best use of ongoing monitoring procedures or lacked necessary monitoring procedures altogether, which may have caused them to implement inefficient year-end evaluations to support their conclusions about the effectiveness of internal control.

4. This *Guidance on Monitoring Internal Control Systems* (COSO’s Monitoring

COSO’s 2006 Guidance
<p><b>Principle 19:</b> “Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.”</p> <p><b>Principle 20:</b> “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.”</p>

Guidance) is intended to help any organization design, implement and evaluate monitoring procedures that achieve the principles of the monitoring component in an effective and efficient manner. It is intended to reinforce and clarify, not add to or change, the sound principles of monitoring previously established through the 1992 COSO Framework and COSO’s 2006 Guidance.

5. This guidance is designed to apply to all three objectives addressed in the COSO Framework: the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. However, recognizing that the primary application of this guidance may be related to monitoring internal control over financial reporting (ICFR), most of the examples included herein concentrate on the financial reporting objective.

### Role of Monitoring

6. In an effective internal control system, the COSO Framework’s five components work together, providing **reasonable assurance** to management and the

board of directors<sup>4</sup> regarding the achievement of the organization’s objectives.<sup>5</sup> The monitoring component helps ensure that the internal control system continues to operate effectively. As such, the effective operation of the monitoring component provides value to the organization in three ways:

- It enables management and the board to determine whether the internal control system — including all five components — continues to operate effectively over time. Thus, it provides valuable support for assertions, if required, about the internal control system’s effectiveness.
- It improves the organization’s overall effectiveness and efficiency by providing timely evidence of changes that have occurred, or might need to occur, in the design or operation of internal control, thus helping the organization to identify and correct control deficiencies *before* they **materially** affect the internal control system’s ability to achieve the organization’s objectives.
- It promotes good control operation. When people who are responsible for internal control know their work is subject to oversight through monitoring, they are more likely to perform their duties properly over time.

**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.”

7. Properly designed and executed monitoring requires planning that leads to the evaluation of **persuasive information**, which is both **suitable** and **sufficient** in the circumstances.<sup>6</sup> In contrast, ineffective monitoring, over time, allows the natural deterioration of internal control systems. Controls within any or all of the five components may change, cease to operate or lose effectiveness because of changes in circumstances. Accordingly, monitoring should be designed to identify and evaluate such changes in a timely fashion.

<sup>4</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 stakeholders who serve in a governance and oversight capacity. For simplicity, this guidance will use the terms “board of directors” or “board” to refer to all groups charged with governance and management oversight.

<sup>5</sup> COSO Framework, p. 15.

<sup>6</sup> See the discussion of persuasive information beginning on page 29.

8. A system of internal control cannot guarantee the achievement of organizational objectives, and monitoring cannot guarantee the prevention or detection of all control deficiencies. However, when properly designed and executed, monitoring does provide support for a reasonable conclusion about the effectiveness of the internal control system.

9. Monitoring considers how the *entire* internal control system manages or mitigates risks to achieving the organization's objectives. Its effectiveness and efficiency are enhanced when it draws from the conclusions reached in the risk assessment component, allowing the organization to design monitoring procedures that are commensurate with the level of risk. Organizations further enhance monitoring's effectiveness and efficiency by selecting controls<sup>7</sup> to monitor based on the level of support they are likely to provide regarding conclusions about the internal control system's effectiveness. In contrast, monitoring is less effective and efficient when it focuses on a checklist of control activities that are selected for evaluation without regard to (1) the level of the risk they address, or (2) the amount of support they provide.

10. Many organizations will find that the elements of monitoring described in this guidance are part of their routine activities. This guidance will help them identify and more effectively utilize existing monitoring (e.g., to provide support for external assertions regarding internal control effectiveness). Other organizations may find that they lack effective monitoring or perform monitoring in an inefficient manner. This guidance will help them improve their monitoring procedures.

## Structure of Effective Internal Control Systems

11. 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>8</sup>

---

<sup>7</sup> Throughout this guidance, the terms "internal controls" and "controls" are used to refer to the control processes and elements put in place to achieve the objective of *any of the five* COSO Framework components. The term "control activities" refers specifically to internal controls that achieve the objective of the COSO Framework's *control activities* component.

<sup>8</sup> COSO Framework, p. 13.

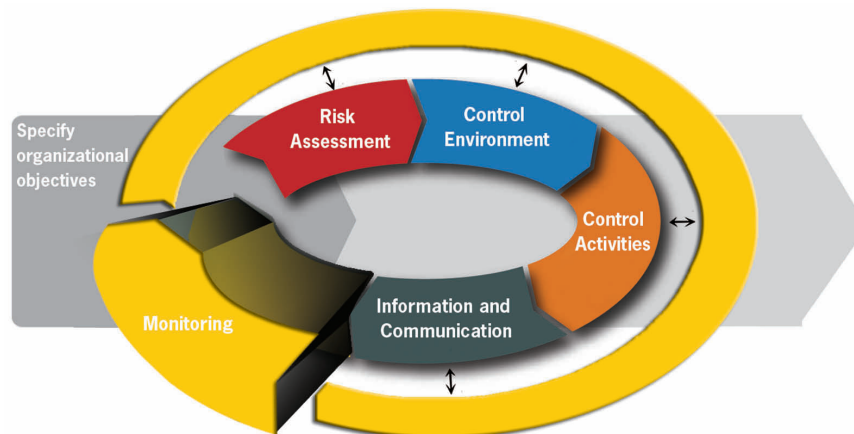


12. Organizations achieve these objectives through the operation of the five interrelated components of internal control. These components provide a framework for understanding internal control and assessing its effectiveness.

13. The concepts embodied in the COSO Framework are frequently presented in the form of a three-dimensional cube (see page 1, Figure 1) that depicts the five components operating *across* each internal **control objective**<sup>9</sup> and *within* all organizational units and activities.

14. Not only does the cube demonstrate 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 controls or process owners — often monitor by evaluating the results of monitoring activities performed at another level. Conversely, in smaller organizations, management often has more direct exposure to the operation of controls and, thus, might rely less on monitoring performed by others.

15. The interrelationships embodied in the components of the COSO Framework have also been illustrated in the process-oriented graphic included in COSO’s 2006 Guidance. This graphic (modified in Figure 2) depicts the monitoring component as a process that evaluates the internal control system’s effectiveness, in its entirety, in managing or mitigating **meaningful risks** to organizational objectives. This process



Monitoring Applied to the Internal Control Process  
**Figure 2**

<sup>9</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.

view of the COSO Framework demonstrates that monitoring does not seek to conclude on the effectiveness of individual internal control components operating in isolation.

16. This view also shows that internal controls<sup>10</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, and
4. Designing and implementing responses to the risks (e.g., internal control).

17. Many organizations design and implement monitoring procedures in conjunction with step #4 above. Doing so allows the organization to utilize the results of the risk assessment process to facilitate the design of the entire internal control system, including monitoring activities. However, monitoring activities can be designed or adjusted *after* other elements of the internal control system have been implemented.

18. In order to implement monitoring that provides the necessary level of support, organizations must make several decisions. Some of those key decision points — and the paragraphs in this Volume in which they are discussed — are listed below.

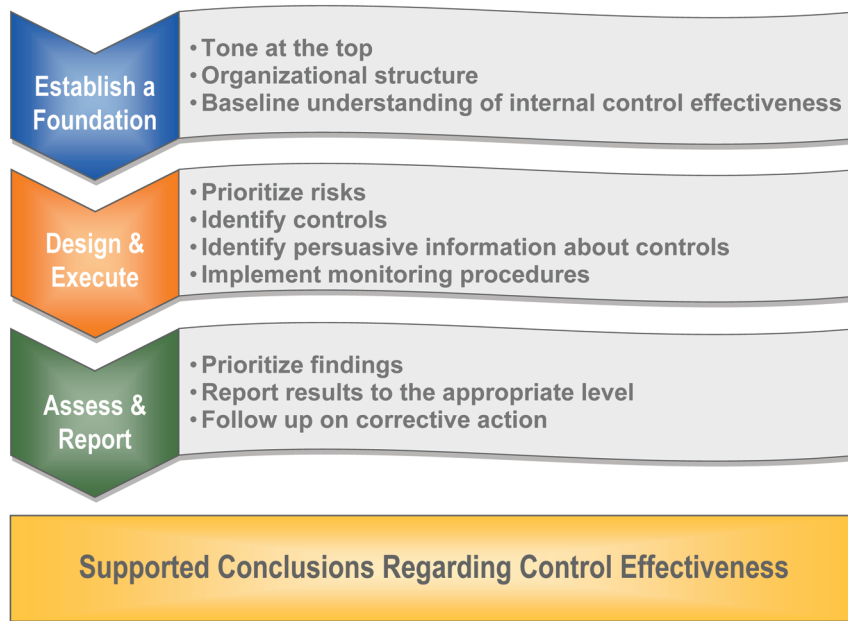
Who should perform monitoring	Paragraphs 27–37
What controls to consider	Paragraphs 54–62
What information to evaluate	Paragraphs 63–83
What procedures to employ and how often	Paragraphs 84–93
How to assess and report results	Paragraphs 94–107

19. This list and the following model for monitoring are not meant to prescribe an order of events, but to portray monitoring within an organization as a dynamic and continually evolving process.

---

<sup>10</sup> See footnote 7 on page 4.

### A Model for Monitoring



The Monitoring Process  
**Figure 3**

20. Management implements monitoring by (see Figure 3):
  1. Establishing a foundation for monitoring, including:
    - A tone at the top that stresses the importance of monitoring,
    - An effective organizational structure that considers the roles of management and the board in regard to monitoring, and places people with appropriate capabilities, objectivity, authority and resources in monitoring roles, and
    - A baseline understanding of internal control effectiveness.
  2. Designing and executing monitoring procedures that:
    - Evaluate controls in areas of meaningful risk,
    - Select appropriate controls for evaluation from across any or all of the five components,
    - Identify information that will be persuasive in supporting conclusions about control effectiveness, and
    - Evaluate that information through a mix of ongoing monitoring and separate evaluations.



3. Assessing and reporting results in order to:

- Prioritize findings,
- Provide support at the appropriate organization level for conclusions regarding the effectiveness of internal control, and
- Facilitate prompt corrective actions<sup>11</sup> and follow-up where necessary.

21. As noted above, the intent of this model is not to dictate exact monitoring procedures, but to articulate the general flow of monitoring in a dynamic environment as envisioned in the 1992 COSO Framework. The table in Appendix B demonstrates how this model links to that Framework.

---

<sup>11</sup> Correcting deficiencies may be considered a management activity rather than an element of internal control (see the COSO Framework, page 21, Exhibit 3). Regardless of how it is classified, correcting control deficiencies should take place when the organization determines that control deficiencies are severe enough to warrant correction.

## II. Establish a Foundation for Monitoring

22. The foundation for monitoring includes (1) a tone at the top about the importance of internal control (including monitoring), (2) an organizational structure that considers the roles of management and the board in regard to monitoring and the use of **evaluators** with appropriate capabilities, objectivity, authority and resources, and (3) a baseline understanding of internal control effectiveness.

### Tone at the Top

23. As with every internal control component, the ways in which management and the board express their beliefs about the importance of monitoring have a direct impact on the effectiveness of internal control. Management's tone influences the way employees conduct and react to monitoring. Likewise, the board's tone influences the way management conducts and reacts to monitoring.

#### Applying the Concepts — Tone at the Top<sup>12</sup>

Expressing a positive tone at the top regarding internal control and the importance of monitoring involves communicating expectations and taking action when necessary.

- Communicating expectations — Personnel responsible for key areas of operations, financial reporting or compliance should understand that management expects them to (1) know the risks in their area of responsibility that can materially impact organizational objectives, and (2) monitor controls designed to manage or mitigate those risks. Expectations can be emphasized in periodic meetings or performance reviews, or may be written into job descriptions. As organizations grow in size, these communications may need to be more formalized.
- Taking action — When control problems are identified, the action required of management and the board depends on the circumstances. It could involve discussions with responsible parties, training, redesign of controls or monitoring activities, or discipline. By taking appropriate action — especially when deficiencies or their consequences are significant — management and the board send a strong message throughout the organization about the role of monitoring and the importance of internal control.

<sup>12</sup> Throughout this document, the sections titled “Applying the Concepts” provide users with an easy reference as to see how they might employ the ideas presented.

## Organizational Structure

24. Monitoring involves establishing appropriate roles and responsibilities of management and the board regarding monitoring and placing evaluators with proper characteristics in the right positions.

### *Role of Management and the Board*

25. As noted earlier, management has the primary responsibility for the effectiveness of an organization's internal control system. Management establishes the system and implements monitoring to help ensure that it continues to operate effectively. The board's role is one of oversight. For publicly listed companies, the board's responsibilities may be mandated by law, listing-exchange requirements or charter. For privately held and not-for-profit organizations, the board's responsibilities typically are listed in the board's charter.

26. Relative to monitoring, the board exercises its oversight responsibility by understanding the risks to organizational objectives, the controls that management has put in place to mitigate those risks, and how management monitors to help ensure that the internal control system continues to operate effectively. For controls that members of senior management may not be able to monitor objectively— such as those that they perform directly or those that address the risk of senior-management override — the board may determine that someone else with an appropriate level of objectivity should perform monitoring procedures. Such monitoring is often accomplished through an internal audit function or through other objective senior-management personnel.

### **Applying the Concepts — Organizational Structure**

In order to perform its oversight function the board need not understand all of the details of every monitoring procedure. Sources of information that may persuade the board that management has implemented an effective monitoring system include (1) inquiries and observation of management, (2) the internal audit function (if present), (3) hired resources or specialists (when necessary), and (4) external auditors. The board might also consider the information from ratings agencies and analysts. Finally, in some circumstances, boards might make inquiries of non-management personnel, customers and/or vendors.

An effective internal audit function can be a valuable tool for the board in exercising its oversight role. In small organizations, however, the board may not have access to an internal audit function and may need to increase its oversight efforts, especially in areas lacking management objectivity. Board members may decide to increase their interaction with non-management personnel or observe some controls in operation (notably, controls in areas of higher risk). As organizations grow in size and complexity, they may need internal auditors or other experts to help evaluate the effectiveness of the internal control system in certain areas.

COSO's 2006 Guidance, which focused on internal control over financial reporting, contains some useful attributes of Principle 2 regarding the role of the board of directors. Principle 2 says, "The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control." Three attributes of that principle relate to the board's oversight role regarding monitoring:

- **Monitors Risk** — The audit committee actively evaluates and monitors risks of management override of internal control and considers risks affecting the reliability of financial reporting.
- **Oversees Quality and Reliability** — The audit committee provides oversight to the effectiveness of internal control over financial reporting and financial statement preparation.
- **Oversees Audit Activities** — The audit committee oversees the work of both internal and external auditors and interacts with regulatory auditors if necessary. The audit committee has exclusive authority to engage, replace and determine the compensation of the external audit firm. The audit committee meets privately with internal and external audit to discuss relevant matters.<sup>13</sup>

If the external auditor's work or regulatory examinations identify errors or control deficiencies, the organization should consider those results in the context of its own monitoring (i.e., identifying the root cause of the errors or control deficiencies, prioritizing any control deficiencies based on severity, and reporting the results to people who are in a position to take any necessary corrective action). However, management should not plan to reduce its monitoring — and the board should not decrease its oversight efforts — in other areas simply because the external auditor or regulator did not find errors or control deficiencies.

---

<sup>13</sup> See COSO's 2006 Guidance, page 23.

### Characteristics of Evaluators

27. The monitoring process involves people who are responsible for determining what and how to monitor, assessing the monitoring information and reaching a conclusion regarding the effectiveness of internal control. This guidance refers to such people as “evaluators.” Evaluators can be specially trained professionals separate from operations (e.g., internal auditors) or people within the organization who, as part of their routine job function, are responsible for overseeing processes or monitoring the operation of certain controls. Regardless, in order to design and implement monitoring procedures, evaluators require adequate skills, authority and resources, as well as an understanding of the risks that the controls are intended to manage.

28. The right side of the COSO Framework cube (see Figure 4) illustrates how internal control systems, including monitoring, might be viewed across an organization. It also demonstrates that individuals serving in different capacities within an organization may have some monitoring responsibility.

29. Some people who are not responsible for designing or executing monitoring procedures 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 may provide information that is used by a regional manager to perform the monitoring function. These personnel are vital to



The COSO Internal Control  
Integrated Framework  
**Figure 4**

constitutes a control deficiency. Monitoring includes the identification of control deficiencies (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 as to how the internal control system operates can be useful in that regard.

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

30. Both evaluators and their information sources (i.e., the people responsible for providing information to evaluators) need to be appropriately **competent** and **objective**.

31. Competence refers to the evaluator’s knowledge of the internal control system and related processes, including how controls should operate and what

32. As to the competence of information sources, people who provide monitoring information to evaluators should know how to compile complete and accurate information.

33. Objectivity refers to the extent to which evaluators and information sources can be expected to perform an evaluation or provide information with no concern about possible personal consequences and no vested interest in manipulating the results for personal benefit or self-preservation. Personal integrity is a primary consideration in assessing objectivity, but other, more easily observed factors include compensation incentives, reporting responsibilities, personal relationships and the degree to which individuals might be otherwise affected by the results of monitoring.

34. The evaluator’s objectivity can be viewed along a continuum from least to most objective (see Figure 5). **Self-review**<sup>14</sup> (the evaluation of one’s own work) is least objective and, thus, is limited in its ability to support conclusions about the effectiveness of internal controls. Self-review can, however, serve a valuable role in an internal control system since it naturally occurs close to the point of control execution and usually affords the first opportunity to identify control deficiencies before they can become material to the organization.



Objectivity in Assessment  
**Figure 5**

35. Peer review, which is more objective than self-review, is the evaluation of a coworker’s or peer’s work. Supervisory review is the evaluation of a subordinate’s work and is typically more objective than peer review. 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. As a result, they are in the best position to identify and correct control deficiencies promptly.

<sup>14</sup> The term “self-review” in this document refers narrowly to the review of one’s own work. It represents the least objective form of “**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.



36. 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.

37. On a relative basis, senior management in small organizations may be more directly involved in the operation of controls than it is in large organizations. This direct involvement can be advantageous in that it provides senior managers in small organizations with highly persuasive information to support their conclusions about the effectiveness of internal control. However, their direct involvement also diminishes their objectivity in monitoring, which — depending on the level of risk — may increase the importance or change the nature of the board’s monitoring activities.

#### Applying the Concepts — Characteristics of Evaluators

Management might consider a two-step process to place people with the right capabilities, objectivity, authority and resources into monitoring positions. The first step is to establish monitoring leadership at the executive level, which, for illustrative purposes, might start with the:

- Chief financial officer (CFO) and controller responsible for monitoring internal control over financial reporting;
- Chief information officer responsible for monitoring controls over information systems; and
- Chief risk officer or chief legal officer responsible for monitoring controls over compliance with laws and regulations.

The people responsible for executive-level monitoring should have an understanding of the risks that affect the achievement of the organization’s objectives and possess the skills to manage those risks.

Monitoring leadership can then match the skills and objectivity needed by evaluators with the controls that require monitoring. For example, complex areas may warrant monitoring by evaluators that have specialized skills or training. Processes that directly impact people’s compensation, or that might otherwise be subject to theft or fraud, typically warrant evaluators that have a high degree of objectivity. Internal audit often can provide valuable insight in determining who should monitor controls over risks in a given area.

The board could consider this same two-step process in determining an appropriate approach to its monitoring activities. The possible outcome of the process includes directing internal audit or others to perform monitoring procedures in certain areas or directing independent board members with appropriate expertise to perform monitoring.

## Baseline Understanding of Internal Control Effectiveness

38. Internal control systems fail because:

- They are not designed and implemented properly at the outset;
- They are designed and implemented properly, but the environment in which they operate changes, (such as through changes in risks, people, processes or technology) and the design of the internal control system does not change accordingly; and/or
- They are designed and implemented properly, but their operation changes in some way, rendering them ineffective in managing or mitigating applicable risks.

39. In all three circumstances, a baseline understanding of the internal control system's effectiveness in a given area can serve as a starting point for monitoring. Such a baseline allows organizations to design monitoring procedures (ongoing and separate evaluations) to address changes in "real time" by identifying those that (1) should be made in the operation of controls, or (2) have already occurred, enabling evaluators to confirm that they were managed properly. Accordingly, monitoring can be viewed at a high level as following this general sequence (illustrated in Figure 6):

- *Control Baseline* — Monitoring starts with a supported understanding of the internal control system's design and of whether controls have been implemented to accomplish the organization's internal control objectives. As management gains experience with monitoring, its baseline understanding will expand based on the results of monitoring. If an organization does not already have such a baseline understanding in an area with meaningful risks, it will need to perform an initial, and perhaps extensive, evaluation of the design of internal control and determine whether appropriate controls have been implemented. Figure 6 shows the control baseline as the starting point and a new control baseline established over time through monitoring.
- *Change Identification* — The risk assessment component<sup>15</sup> of internal control identifies changes in processes or risks and verifies that the design of underlying controls remains effective. Monitoring, through the use of ongoing and separate evaluations,<sup>16</sup> should consider the risk assessment component's ability to identify and address those changes. Monitoring also identifies indicators of change in the design or operation of controls and

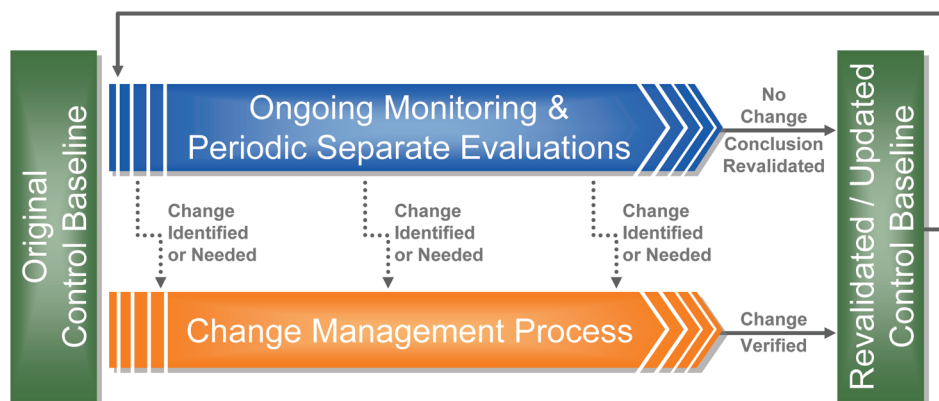
<sup>15</sup> Chapter 3 of the 1992 COSO Framework discusses the risk assessment component. On p. 44 it states, "Fundamental to risk assessment is a process to identify changed conditions and take action as necessary."

<sup>16</sup> See Ongoing Monitoring and Separate Evaluations on page 40 for further discussion.

verifies that the controls continue to meet their objective of helping to manage or mitigate related risks.

Figure 6 demonstrates how ongoing monitoring and periodic separate evaluations can identify changes or, when no changes are present, revalidate the conclusion that controls are effective (see Control Revalidation/Update below).

- *Change Management* — When changes in the operation of controls have occurred, or when needed changes in control design are identified, monitoring verifies that the internal control system manages the changes and establishes a new control baseline for the modified controls.
- *Control Revalidation/Update* — When ongoing monitoring procedures use persuasive information,<sup>17</sup> they can routinely revalidate the conclusion that controls are effective, thus maintaining a *continuous* control baseline. When ongoing monitoring uses less-persuasive information, or when the level of risk warrants, monitoring periodically revalidates control operation through separate evaluations using appropriately persuasive information.



Monitoring for Change Continuum  
**Figure 6**

40. This broad depiction of monitoring is intended to demonstrate how monitoring of a known effective internal control system is a process that looks for and evaluates changes that may have a bearing on its effectiveness. It is not intended to dictate monitoring procedures or a documentation format.

<sup>17</sup> See the discussion of persuasive information beginning on page 29.

41. Note that the four elements described in paragraph 39 do not reside solely within the monitoring component. For example, the risk assessment component might be considered chiefly responsible for identifying changes in the operating environment. Likewise, evaluating the design and implementation of changes in internal control might be considered a control activity. The monitoring component operates to help ensure that the other components are identifying and managing changes that may affect internal control. The next chapter demonstrates how monitoring can be designed and executed to achieve these broad goals of identifying changes from the baseline and verifying that the changes were managed properly.

### Applying the Concepts — Baseline Understanding of IC<sup>18</sup> Effectiveness

The following example demonstrates how ordinary supervisory activities can be part of monitoring.

Assume that a supervisor is responsible for multiple order-entry personnel and is concerned about the completeness, accuracy and timeliness of orders entered into the sales system. He or she begins the monitoring process with (1) an understanding of how the internal control system manages or mitigates the risks that might lead to incomplete, inaccurate or untimely order entry, and (2) a basis for believing that those controls are effective (i.e., a control baseline).

From that baseline, the supervisor could then develop ongoing monitoring procedures that identify changes in the environment or control operation. Monitoring for changes in the *environment* might include the routine business practice of considering the implications of new sales channels or of changes in the order-entry system programming.

Monitoring for changes in *control operation* might include routine reviews of order-entry statistics (e.g., orders entered per person or system edit reports showing keying-error statistics). It might also include periodic observation of orders being entered or re-verification of selected orders within the order-entry team.

This combination of monitoring procedures can operate as a routine part of business operations. If the supervisor identifies a change, he or she can verify that the change was handled appropriately and possibly, for a time, increase the scope of monitoring of controls affected by the change. For example, if the organization added a new sales channel with different order-entry procedures, the supervisor might verify that the new procedures are designed and implemented properly (i.e., change management). He or she might then decide to perform, for some period of time, more-robust observation of the new orders being entered and/or select more orders for re-verification than would be selected of the older, routine orders.

Thus, the effective change-identification and change-management procedures can draw attention to areas of heightened risk due to change, allowing the supervisor to

<sup>18</sup> IC is the acronym for “internal control.”

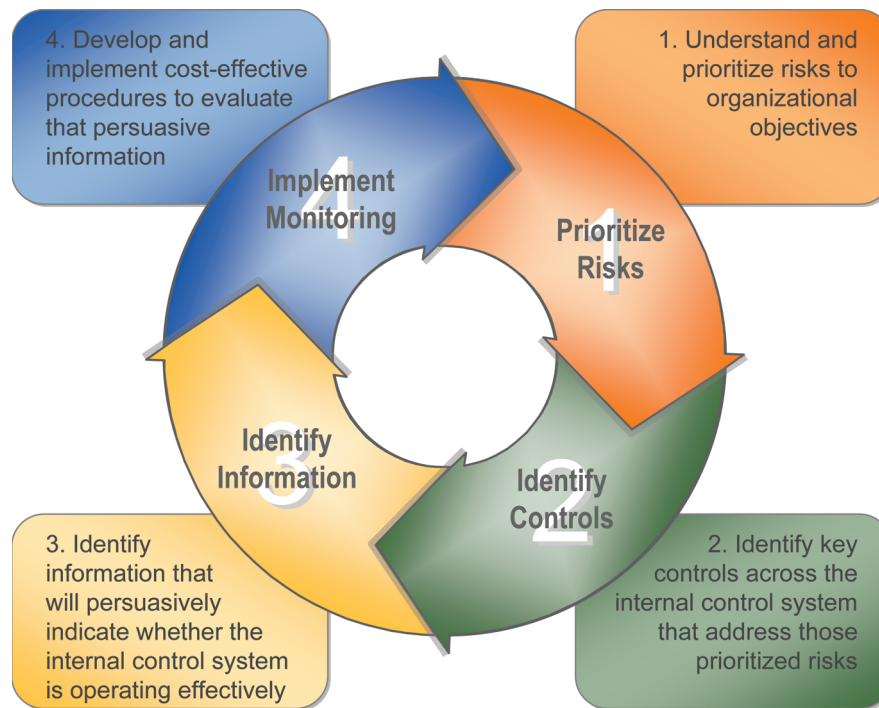
vary the type, timing and extent of monitoring procedures — thereby improving their overall efficiency.

Absent any changes, and assuming the ongoing monitoring procedures do not already provide the level of support needed over a long period of time, the supervisor would, at some point, revalidate that order-entry controls are operating correctly. Such revalidation would occur periodically, commensurate with the level of risk.

### III. Design and Execute Monitoring Procedures

42. Monitoring should enable evaluators to assess persuasive information about the operation of one or more controls that address meaningful risks to the organization’s objectives for which they are responsible. It is risk-based, enabling evaluators to focus their monitoring efforts on that which will provide adequate support for their conclusions about the internal control system’s effectiveness.

43. Evaluators might consider designing monitoring by following the logical progression demonstrated in Figure 7. Note, however, that this progression is not meant to imply a rigid, compartmentalized monitoring process where each step starts and stops before the next. Monitoring is a dynamic process and each of these “steps” operates, to some extent, at all times. This graphic and the discussion that follows are intended to portray the general flow of monitoring in practice.



Monitoring Design and Implementation Progression

**Figure 7**

44. The components in this illustration are discussed in detail in later sections, but the following summary may be helpful.

45. Monitoring is risk-based when it focuses on the evaluation of controls that address meaningful risks to an organization's objectives.

### **1** Prioritize Risks

Meaningful risks are those that, in a given time frame, might reasonably have a consequential effect on organizational objectives.

46. Meaningful risks may vary between similar organizations and between different levels within the same organization. For example, controls that mitigate the risk of supplies theft may fall within the monitoring responsibilities of a retail chain store manager, but may not warrant the frequent attention of the chief executive officer in the context of his or her organization-wide responsibilities.

47. Risk prioritization is a natural part of the risk assessment component of internal control. Its inclusion here is not meant to imply the need for a separate risk assessment function dedicated solely to supporting monitoring. In a properly operating internal control system, the risk assessment component will routinely identify and prioritize risks to the organization's objectives. The results of that process will then influence decisions regarding the type, timing and extent of monitoring.

48. Controls that address meaningful risks are then selected for evaluation based on their ability to provide support for a reasonable conclusion about the internal control system's effectiveness. Such controls, referred to as **key controls** in this guidance, may operate within any or all of COSO's five components.

### **2** Identify Controls

49. Selecting *key controls* that address *meaningful risks* enhances the effectiveness and efficiency of monitoring by focusing on that which provides an adequate but not excessive level of support for a conclusion about the internal control system's effectiveness.

50. Organizations can identify key controls<sup>19</sup> by (1) understanding how the internal control system is designed to manage or mitigate meaningful risks, and (2) determining which controls will contribute most to the monitoring conclusion. Key controls often have one or both of the following characteristics:

- Their failure could materially affect the objectives for which the evaluator is responsible, but might not be detected in a timely manner by other controls, and/or

<sup>19</sup> Key controls can include controls from any of the five COSO components, not just control activities.



- Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization’s objectives.

51. Identifying key controls is not meant to suggest that they are necessarily more important to the internal control system than other controls. It is merely intended to help organizations devote monitoring resources where they can provide the most value.

52. Once key controls are selected, evaluators identify the information that will support a conclusion about whether those controls have been implemented and are operating as designed. Identifying this information entails knowing how control failure might occur and what information will be persuasive in determining whether the control system is or is not operating effectively.

**Identify Information**

53. The identification of persuasive information allows the organization to determine which monitoring procedures to employ (i.e., ongoing monitoring, separate evaluations, or a combination of both), as well as the frequency with which the monitoring procedures should take place.

**Implement Monitoring**

### Prioritize Risks

54. As part of the risk assessment component of internal control,<sup>20</sup> management identifies and evaluates risks to achieving the organization’s objectives. This process enables the organization to design an effective internal control system, which includes all five components of internal control.

55. Initially, risk assessment might involve a comprehensive analysis of objectives and the risks that could have a meaningful effect on the achievement of those objectives. This process includes considering risks that may manifest at the entity level or at the activity level.<sup>21</sup>



56. The formality and frequency of risk assessment can vary greatly among organizations. A large, complex organization might perform annual or more-frequent assessments using complex risk-scoring mechanisms. Conversely, a small, non-complex organization might update its risk assessment through

<sup>20</sup> 1992 COSO Framework Chapter 3, COSO’s 2004 Enterprise Risk Management — Integrated Framework (COSO ERM), Chapters 5–6, and COSO’s 2006 Guidance, Chapter II, provide useful guidance regarding risk assessment and risk response.

<sup>21</sup> 1992 COSO Framework, Chapter 3 contains examples of both levels of risk and discusses ways to conduct risk analysis.

discussions among knowledgeable people, performing its updates less frequently unless changes in the environment dictate otherwise. Regardless, the assessment considers the importance of the risk *without* considering the expected effectiveness of internal control. For example, in prioritizing risks related to revenue recognition, an organization's initial assessment of the channel-stuffing<sup>22</sup> risk as "low" — based on the expectation that the internal control system will prevent or detect such activity — could lead to the inappropriate exclusion of important controls from monitoring. Considering risk importance apart from expected control effectiveness helps ensure that the organization monitors controls it relies on most to address meaningful risks.

57. For each objective and risk, the organization might identify locations, operations or processes where manifestation of the risk could be material.

58. Risk factors to consider at this stage include:

- Nature of operations — The way an organization is structured and the characteristics of its operations can influence the need for and conduct of monitoring. Such characteristics might include, but are not limited to, transaction volumes, operational complexity, dollar amounts involved, geography, degree of centralization, information system complexity and existence of foreign operations.
- Changes in operations — Mergers, joint ventures, acquisitions, system changes, personnel and other changes are indicators of increased risk.
- Environmental factors — The external environment can affect an organization's viability and increase the need to monitor certain internal controls. External risk examples include competition, changes in the market (e.g., technology, supply chain, customer base or economy), regulation, and areas with a heightened risk of litigation or loss.
- Susceptibility to theft or fraud — Some factors can increase the potential for theft or fraud. Examples include: the presence of valuable assets (e.g., cash, trade secrets, fungible goods); employee performance metrics that may provide an incentive to commit fraudulent acts; and process or system designs that make theft or fraud possible through access to systems, execution of unauthorized transactions and/or override of controls. The presence of such risk factors increases the need for strong internal controls and related monitoring.


---

<sup>22</sup> Channel stuffing is the business practice of inflating sales figures by pushing more goods through a distribution channel than it has the capacity to sell or use. Revenues are improperly inflated for a period, with the excess goods being returned to the company at a future date.

### Applying the Concepts – Prioritize Risks

Assume that management of a manufacturing organization wants to be confident that internal control over financial reporting is effective. Management can begin the analysis by reviewing its financial statements and asking what can go wrong or what might reasonably prevent the organization from achieving its financial reporting objectives in a given area. The following revenue recognition example may clarify the thought process.

Note: This example is not designed to show all revenue recognition risks, nor is it intended to establish a standard risk-importance grade. Reasonable people, given the same set of facts, might reach different conclusions regarding risk prioritization and, later, regarding key control selection and other monitoring decisions.



1. Prioritize Risk			
Area	Objective	Risk	Priority
Revenue	1. Recognize in the proper period	Overstatement – recording revenue before delivery or title transfer	Moderate

Rationale:

Factors increasing risk:

- This organization’s quarter-end sales and shipping activity is typically high, increasing cutoff risk
- Dollar amounts involved at or near quarter-end for this organization are normally material to the financial statements
- The compensation plan is structured such that it could influence sales personnel to push for premature recognition

Factor decreasing risk:

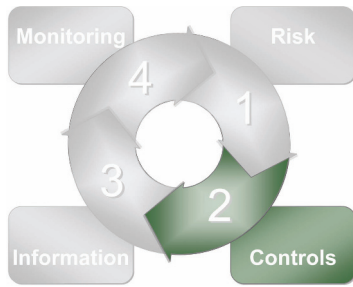
- The organization’s standard business practice requires FOB-shipping-point terms, thus reducing cutoff risk related to the issue of title transfer

This same organization might rate a different revenue-related risk as having a higher priority, as the following channel-stuffing example demonstrates. (Note: This channel-stuffing example will be expanded further throughout the remainder of the guidance.)

Area	Objective	Risk	Priority
Revenue	2. Recognize revenue in proper amounts	Overstatement – sales agents grant future credits for unsold goods (i.e., “channel stuffing”)	High
<p>Rationale:</p> <p>In this example, the monetary amounts involved are material, and this risk is prevalent in the industry. In addition, the company’s compensation plan, which is standard in the industry, could encourage channel stuffing because it rewards sales personnel for sales recorded in a given period. Management also notes that channel stuffing can be very hard to detect in a timely manner, particularly if the sales personnel enter into side agreements with their customers.</p>			
<p>Note that the personnel responsible for this risk assessment process first identified the objectives and the risks to achieving those objectives. Then they thought rationally about the risk, considering factors that might increase or decrease the likelihood and/or significance of the risk.</p>			

### Identify Key Controls

59. In order to identify key controls to monitor, the people designing monitoring procedures must first understand (1) how the internal control system is designed to manage or mitigate the identified meaningful risks, and (2) how that control system could fail, with the failure not being detected in a timely manner.



60. Key controls might include those that represent the most likely point of failure regarding meaningful risks. Other controls may be identified as key because their operation can prevent other control failures, or can detect and correct other control failures before they can become material to

the organization. An example might include a three-way match between purchase order, receiving document and invoice, which can detect certain control failures that occur earlier in the processes associated with purchasing, receiving and accounts payable.

61. Key-controls determination can occur at various levels within an organization. For example, controls that are key in addressing a risk that is meaningful to a plant manager may not be key to senior management in addressing risk at the overall organization level. As evaluators, the plant manager’s and senior management’s roles and purposes for monitoring differ, as do the controls each identifies as key. Accordingly, they will select controls to monitor that will provide them with the necessary level of support commensurate with their roles and responsibilities.

62. This key-control analysis can be facilitated by considering factors that increase the risk that the internal control system will fail to properly manage or mitigate a given risk. These control risk factors might include the following:

- Complexity — Controls that require specialized skill or training typically are more susceptible to failure than simple controls.
- Judgment — Controls that require a high degree of judgment, such as controls over the determination of valuation allowances, are highly dependent on the experience and training of those responsible for the judgments and are often associated with meaningful risks.
- Manual vs. automated — Manual controls are more susceptible to human error than automated controls and, as a result, are often subjected to different levels of monitoring than automated controls (e.g., they may be evaluated more frequently or employ larger sample sizes when sampling is performed). However, when automated controls fail, they tend to fail repeatedly in the same circumstances and, therefore, need to be subjected to an appropriate level of monitoring when they address meaningful risks. The table on page 35 contains some additional guidance about monitoring manual and automated controls.
- Known control failures — Previous control failures are a clear indicator of the need to increase monitoring activities until corrective actions have effectively addressed the cause of the control failure.
- Competence/experience of personnel — Lack of qualifications or experience in performing a given control increases the likelihood of control failure.
- Risk of management override — Controls that might be overridden by management for purposes that are contrary to organizational objectives may warrant specific monitoring attention.
- Likelihood of control failure detection — Other controls within the internal control system may reasonably be expected to detect a given control's failure before it becomes material, decreasing the need to identify the given control as key. Conversely, a reasonable belief that a control's failure may be material, and not detected and corrected on a timely basis, increases the need to identify the control as key.

### Applying the Concepts — Identify Key Controls

Continuing the revenue recognition example from page 23, the organization might identify key controls addressing the risk of channel stuffing through a process similar to the one outlined below.

This control-identification process might vary from organization to organization; however, in every organization, it is essential that the personnel responsible for designing monitoring first understand how the internal control system addresses the

risk at relevant locations or levels within the organization. They can then identify the controls that will provide the necessary support to conclude that the internal control system is working.

In the channel-stuffing example, the organization identified 11 controls relevant to mitigating the risk of channel stuffing, with four of them selected as “key” controls (see the following table). The rationale for selecting each key control is presented below the control, as is the rationale for *not* designating some of the other controls as key. From the perspective of the total internal control system, the evaluator might reasonably conclude that monitoring these four controls will provide adequate support for conclusions about the whole system’s effectiveness in addressing this risk.

First, some caveats regarding this example:

1. To save space, this table does not include the rationale regarding *all* “non-key” controls and why they were not selected as key.
2. Reasonable people might reach different conclusions regarding which of the controls below are key and which are not. The varying nature of risk and control can lead two organizations to implement controls and monitoring procedures differently. Therefore, the example is not intended to represent a “best practice” for monitoring internal control over the channel-stuffing risk.
3. This example is not meant to imply that the non-key controls will never be monitored. They may be monitored in relation to other risks, or the organization may decide to evaluate them less frequently. For example, it could decide to evaluate policy training every three to five years. Regardless, the people responsible for monitoring controls in this risk area should be aware of how the internal control system addresses the risk and what controls provide the most support for their conclusions that the system is working.
4. The following table is not meant to imply a level of documentation or a format that is necessary to support the identification of key controls.

2. Identify Key Controls		
Key	Control	Component
⚙️	1. Management philosophy and communication against channel stuffing	Control Environ.
Rationale: This tone-from-the-top control was selected as key because the risk is primarily one of integrity. If sales personnel sense that channel stuffing is accepted they are more likely to engage in the practice. Conversely, if they know that it is not only against policy, but against management's expressed desires, then the risk of channel stuffing will be reduced.		
	2. Training on policies	Control Environ. and Info. & Commun.
	3. Code of conduct signed by all sales personnel	Control Environ. and Info. & Commun.
	4. Policies specifically against channel stuffing	Control Activity
	5. Standardized contracts	Control Activity
Rationale: This control might be considered "key," but the effective operation of control #6 would catch its failure on a timely basis. Therefore, this control is not selected as a key control, thus reducing the potential to develop unnecessary monitoring procedures — one of the standardized contract control and another of the standardized contract modification approval control.		
⚙️	6. Sales manager and legal approval required for all modifications of standard sales contracts	Control Activity
Rationale: In this example, the standard contract would have to be modified in order to accommodate channel stuffing. Thus, this approval control would have to fail or be circumvented in order for channel stuffing to occur. As a result, it is selected as a key control. The risk still exists, however, that sales personnel could bypass the standard contract altogether through side agreements with customers. That remaining risk will be addressed by the other selected key controls – in this case, primarily by controls #1, #10 and #11.		



Key	Control	Component
	7. Approval of sales above a certain limit	Control Activity
<p>Rationale:</p> <p>Some controls, such as this sales limit approval control, may address more than one risk and at different levels. For example, this approval control might be a key control related to credit default risks. It also helps address the channel-stuffing risk by limiting a salesperson's ability to sell excessively large quantities to a given customer. However, it is not selected here as a key control related to channel-stuffing risk because (1) an excessively large shipment to a customer would still require modification of credit terms in order to result in channel stuffing (addressed by control #6), and (2) unusually large sales and related returns would likely be identified by key controls #10 and #11.</p>		
	8. Exception reports generated and reviewed for any transactions exceeding authorized limits	Control Activity, Info. & Commun., and Monitoring
	9. System controls that prevent billing (and, thus, revenue recognition) unless goods are shipped	Control Activity
⚙️	10. Salesperson compensation is reviewed quarterly by sales manager and adjusted if returns exceed a threshold percentage of their sales. Anomalies are investigated and results are documented.	Control Activity & Monitoring
<p>Rationale:</p> <p>This control serves as both an effective deterrent and a detective control related to channel-stuffing risk. If it operates effectively, the chance of material channel stuffing is significantly reduced. Therefore, it is identified as a key control.</p>		
⚙️	11. Periodic review by the sales manager (weekly) and CFO (monthly) of sales trends and sales return trends by salesperson, by customer	Control Activity & Monitoring
<p>Rationale:</p> <p>This is a dual-purpose control (i.e., a control activity identifying possible revenue recognition errors and a monitoring activity using indirect information) that <i>might</i> identify a control breakdown in a timely manner. Since any significant channel stuffing by a salesperson would stand out in this trend analysis, it is selected as a key control.</p>		

### Identify Persuasive Information

63. Persuasive information is capable of providing adequate support for a conclusion regarding the effectiveness of internal control. Persuasive information is both *suitable* and *sufficient* in the circumstances and gives the evaluator reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of the internal control system in a given risk area. An appropriate cost-benefit analysis — one that weighs the effort to gather the information against the ability of the information to persuade the evaluator that the controls continue to operate effectively — is an important part of effective, sustainable monitoring. This analysis is normally qualitative in nature, but may contain quantitative measurements as well. Regardless of the method, those responsible for monitoring must exercise judgment in determining the information necessary to have reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of the internal control system in a given area.



64. Suitable information is a broad concept that implies that information is useful within the context for which it is intended. In order to be suitable, information must be **relevant**, **reliable** and **timely**. Sufficiency is a measure of the quantity of information (i.e., whether the evaluator has *enough* suitable information).

### Suitable Information

65. Figure 8 demonstrates how the three elements of suitability operate together. In the center of the diagram, where the information is relevant, reliable *and* timely, the evaluator can turn his or her attention to whether sufficient information is available to form a reasonable conclusion.

66. 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. In such circumstances, and as illustrated in Figure 8, additional information is needed to achieve the required degree of suitability.

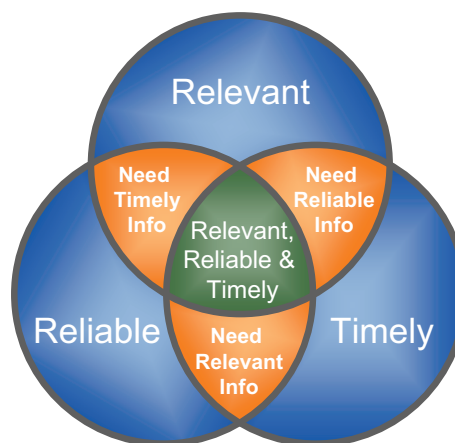
67. Determining the suitability of information being used to evaluate a particular control is a matter of judgment that depends on the level of risk and the internal control system's susceptibility to failure (discussed earlier).

68. *Relevance of information* — Information is relevant when it tells the evaluator something meaningful about the operation of the underlying controls. For example, reviewing résumés and training records can tell an evaluator something about whether an accountant has the background to handle certain areas of complex accounting — the information contained in résumés and training records is *relevant* to the controls regarding the financial competence of personnel.

When evaluators obtain relevant information about the effectiveness of controls, they identify characteristics or attributes indicative of the internal control system's proper performance or failure. They can then test<sup>23</sup> for the presence or absence of these conditions using persuasive direct and indirect information.

69. Information that directly confirms the operation of controls is more relevant than information that requires a greater degree of inference to conclude whether the controls are effective. Using the above example to illustrate this concept, firsthand knowledge that an accountant accurately analyzes complex accounting and makes informed choices (direct information) is more relevant than information obtained by reviewing résumés and training records (indirect information requiring the evaluator to infer that the background and training will lead to more informed analysis and better decisions).

70. **Direct information** substantiates the operation of controls. It is obtained by observing controls in operation,<sup>24</sup> reperforming them, or otherwise evaluating their operation directly, and can be useful in both ongoing monitoring and separate



Elements of Suitable Information  
**Figure 8**

<sup>23</sup> Testing can include such techniques as inspection, observation, inquiry, confirmation, recalculation, reperformance, or analytical procedures.

<sup>24</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. 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 in some situations.

evaluations. Generally, direct information is highly relevant because it provides an unobstructed view of control operation.

71. **Indirect information** is all other information that *may* indicate a change or failure in the operation of controls. It either relates to or is produced by the process in which the controls reside. Indirect information can include, but is not limited to, (1) operating statistics, (2) **key risk indicators**, (3) **key performance indicators**, and (4) comparative industry metrics.

72. Monitoring using indirect information identifies anomalies that may signal a control change or failure and subjects them to investigation. Indirect information does not, however, provide an unobstructed view of control operation, thus it is less able than direct information to identify control deficiencies. Existing control deficiencies may not *yet* have resulted in errors significant enough to be identified as an anomaly, or the indirect information may have lost its ability over time to identify anomalies. Indirect information is thus limited as to the level of support (i.e., persuasiveness) it can provide on its own, especially over a long period of time.

73. When evaluators begin with a baseline understanding of internal control effectiveness, established through the use of persuasive direct information, the evaluation of indirect information can be a valuable monitoring tool that may:

- Signal that a change in the environment or control operation has occurred, or
- Supplement the support provided by direct information — sometimes for an extended time frame — regarding the evaluator’s conclusions about control effectiveness.

74. As a result, monitoring using indirect information can influence the type, timing and extent of future monitoring procedures that use direct information.

75. 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 (indirect information). By itself, a review of credit memos that is free of anomalies does not reveal whether controls over billing continue to operate effectively — the controls may be ineffective, but related problems may not have led (at least, not yet) to the issuance of credit memos. However, in the presence of an effective monitoring structure (including a baseline of direct-information support regarding the effectiveness of billing controls and procedures to identify and manage changes in the billing area), the review of credit memo activity may allow the supervisor to conclude that the risk of control failure in the billing area is reduced to an acceptable level, at least for some period of time. This conclusion might then influence the type, timing and extent of other monitoring procedures over controls in the billing area.

76. The following table highlights some factors that may influence an organization’s decisions regarding the amount of direct and/or indirect information to use in

monitoring. Note that these factors, among others, may also influence judgments regarding the sufficiency of information (i.e., how much information the evaluator needs regardless of its type). See the table following paragraph 82 on page 33 for other factors that may influence judgments regarding sufficiency.

Factor to Consider	Possible Impact on the Use of Direct vs. Indirect Information
Potential impact of a control's failure	As the potential impact of a control failure increases, the need to monitor using direct information increases.
Controls that operate in areas with a high degree of change in people, processes or technology versus controls operating in stable areas	Indirect information is typically less able than direct information to identify possible control failures in areas that are subject to a high degree of change. As a result, controls in those areas warrant monitoring using more-direct information. Conversely, controls that operate in stable environments may be better able to employ indirect information in monitoring.
Recent experience with control performance	Known failures of the internal control system's proper management or mitigation of given risks may warrant an increase in evaluation of direct information.
The length of time since the operation of the underlying controls was last validated through persuasive direct information	Over time, indirect information loses its ability to highlight indicators of control failure. Small errors resulting from failed controls, undetected by indirect information, can compound and become material. They also may gradually influence the indirect information, making the underlying control problem harder to detect. Thus, monitoring using indirect information should be reconfirmed periodically through monitoring of direct information.
The relative persuasiveness of the indirect information	The relevance, reliability, timeliness and sufficiency of indirect information have a direct bearing on its contribution to monitoring. In the earlier channel-stuffing example, the review of sales trends and return trends <i>by salesperson, by customer</i> is more likely to identify a control failure than will a review of sales trends solely at the consolidated company level.
The adequacy of the follow-up process	The skills and experience of people responsible for investigating anomalies, and the diligence with which they conduct their follow-up procedures, affect the ability of indirect information to identify a control failure.
Potential effect on the conduct of external audits, regulatory examinations or other external-party evaluations	External parties, such as auditors or regulators, may be required to conduct independent evaluations of an organization's internal control system. Management's use of direct information in monitoring may facilitate such evaluations by reducing the amount of direct information gathered separately by the external parties.

77. *Reliability of information* — Evaluators 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.

78. Although accuracy and verifiability are commonly understood, objectivity of information sources warrants further discussion.

79. The “Characteristics of Evaluators” section discussed the objectivity of evaluators and their sources of information. The objectivity of the information source is the degree to which that source can be expected to provide unbiased information for evaluation. The more objective the information source, the more likely the information will be reliable. For example, notifying information sources in advance that certain instances of a control will be monitored, or directing them to provide supporting documentation in such a manner and time frame that they have an opportunity to review and correct that documentation before it is examined, reduces the information’s objectivity and, therefore, its reliability.

80. *Timeliness of information* — To be suitable, information must be produced and used in a time frame that makes it possible to prevent control deficiencies or detect and correct them *before* they become material to the organization. The “Ongoing Monitoring and Separate Evaluations” section discusses the time frame in which information is used (i.e., the timing of ongoing monitoring and separate evaluations).

81. To be suitable, the information must also relate to the period under consideration. As information ages, it loses its ability to tell the evaluator whether the related controls are operating properly. Likewise, information produced after a control operates may not help support earlier point-in-time conclusions (if such conclusions are necessary). For example, evaluating the operation of a monthly control in March does not tell the evaluator whether that same control was operating the previous December.

### *Sufficient Information*

82. Evaluators must gather *sufficient* suitable information to support a reasonable conclusion about control effectiveness. Sufficiency can refer to how many occurrences of a given control are evaluated (e.g., selecting 30 occurrences from 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. Examples include infrequently operating control activities or controls within other components, such as the control environment, risk assessment, and information and communication. Regardless, the evaluator must exercise judgment in determining whether he or she is evaluating *enough* information. Some factors to consider include the following (note that several of these factors are also among

those listed in paragraph 76 on page 31 regarding the use of direct and indirect information):

Factor to Consider	Possible Impact on the Amount of Information Needed
Potential impact of a control's failure	The potential impact of a control's failure may affect the amount of information needed to conclude that the internal control system is effective in a given area. 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 when necessary (e.g., after the passage of a certain period of time or upon the identification, through the review of indirect information, of a possible anomaly). Alternatively, in high-risk areas, that same evaluator might monitor every reconciliation control every month.
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.
Recent experience with control performance	Known failures of the internal control system to properly manage or mitigate given risks may warrant an increase in the amount or frequency of information gathered for evaluation.
Control frequency	Controls that occur infrequently are often subjected to judgmental selection methods, while those that occur frequently lend themselves to possible statistical sampling methods. In non-statistical selection methods, organizations determine the amount of information to evaluate after considering the level of risk and the importance of the identified control.
Who is conducting the monitoring	If evaluators are routinely involved in or witness the execution of controls (which constitutes direct information about the operation of controls), then their participation is ordinarily sufficient for them to conclude whether the controls are effective. As evaluators become more distant from the operation of the controls they typically need to obtain more information regarding the controls' operation.



Factor to Consider	Possible Impact on the Amount of Information Needed
Corroboration provided by monitoring other controls	If the monitoring of Control A provides at least partial support that Control B is operating effectively, that fact may influence the amount of information required to evaluate Control B. For example, effective monitoring of a three-way-match control between purchase orders, receiving documents and invoices may help support a conclusion that no data-entry errors were made and that data-entry controls over invoices are effective — possibly impacting the scope of monitoring those data-entry controls.
Complex controls	To address the variables in control operation, complex controls may warrant gathering more information than do 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 of controls is a plausible risk, evaluators might gather more information regarding the effective operation of controls.
Manual controls	For manual controls, which are more prone to error than are automated controls, the quantity of information necessary will vary depending on the frequency of a control's operation, personnel turnover, and the experience and training of personnel who perform the controls.
Automated controls	Automated controls generally operate consistently when they exist in a controlled environment. Therefore, a periodic reconfirmation through evaluation of a single instance of a given automated control is often an acceptable monitoring threshold regarding the operation of that control. In such situations, management includes in its monitoring procedures the effectiveness of relevant information technology general controls such as program testing, program security, change-control processes and, perhaps, data security.

83. Evaluators can conclude that they have sufficient suitable information when, based on the evaluation of that information, they can reasonably conclude either that the risk of a control failure material to the organization's objectives is:

- Below the level of reasonable possibility, or
- Above the level of reasonable possibility, leading to an assessment of the severity of the identified deficiency.

### Applying the Concepts — Identify Persuasive Information

The consideration of information suitability and sufficiency in monitoring is not intended to create prescriptive rules for monitoring (e.g., establishing a certain percentage of direct versus indirect information). Rather, it is to help those responsible for monitoring evaluate the level of support that various information sources might provide in a given risk context.

Answering a series of questions may help evaluators make this judgment. Example questions include:

- Is the information relevant to a conclusion about control effectiveness?
- Does the information demonstrate *directly* whether the control being evaluated operates properly, or does it require a greater degree of inference based on the existence or lack of certain anomalies?
- If the indirect information is not negative (i.e., it does not indicate that the control may have failed to operate properly), how supportive is it in light of the:
  - Level of risk the control is intended to mitigate,
  - Length of time since evaluators last obtained information that directly supported their control conclusions, and
  - Effectiveness of other controls that might address the same risk(s)?
- Does the organization have a reasonable basis for concluding that the information used in monitoring is reliable? For example:
  - If the information comes from a system report, are the controls affecting that system report effectively monitored?
  - Does the information come from an objective source, or can it be confirmed by an objective source?
- Is the information possibly subjected to a procedure or reconciliation that might affirm its reliability? (For example, a three-way match of purchase orders, receiving documents and invoices helps support a conclusion that the related dollars and/or quantities are accurate.)

- Is the information evaluated in a time frame that allows the organization to take corrective action before a control breakdown has a reasonable opportunity to materially affect related objectives?
- Does the information relate to the period under consideration? (For example, information may be too old to tell evaluators anything about the current operation of controls, or it might come from a period following the desired control evaluation date.)
- Do evaluators gather and evaluate enough information to support their control conclusions? (Note: the answer might be influenced by some of the factors listed in the table on page 34.)

Continuing the earlier revenue recognition example, the following represents this “level-of-support” thought process. Recall that the organization identified the risk of channel stuffing as “high” and identified four key controls out of 11 that it will subject to specific monitoring procedures. Here, the organization identifies what information is available to support a conclusion about whether those controls are working.

In this example, where the underlying risk relates to a potential material misstatement of the financial statements, the ultimate risk owner is most likely the CFO, and oversight is provided by the audit committee. To the extent that the ultimate risk owner (e.g., the CFO) is involved in or directly witnesses the execution of the key controls, he or she may not need to gather any additional information about the operation of those controls — participation in the control process can provide sufficient relevant, reliable and timely information to support his or her individual conclusions about control effectiveness. However, to the extent that others, such as the audit committee, are not directly involved and require support regarding control effectiveness, they would need to gather and evaluate additional persuasive information either on their own or through others. The following example demonstrates these two different levels of support.

Note: This example is not meant to show the level of documentation necessary to support the identification of persuasive information. It is intended to demonstrate an organization’s possible thought process in determining what information to use in monitoring.

3. Identify Persuasive Information About Key Controls	
Key Control	Available Information
Control #1 – Tone at the top	<ul style="list-style-type: none"> <li>– Management participation and periodic communications in sales meetings, including setting expectations that specifically address this risk</li> <li>– Evidence of corrective actions, if necessary</li> </ul>
<p>Rationale:</p> <p>Relevant – This information is obtained from witnessing or delivering the communications, so it is relevant.</p> <p>Reliable – For those who witness these communications and actions, this is reliable information because they see the control in action. Others (such as the audit committee) may desire to confirm the communications through discussions with relevant personnel.</p> <p>Timely – The observations happen in real time and would be timely.</p> <p>Sufficient – Witnessing these communications and actions would adequately demonstrate the existence of a proper tone at the top.</p>	
Control #6 – Approval for contract modifications	<ul style="list-style-type: none"> <li>– Signed approval noted on modified contract</li> <li>– CFO participation in sales meetings where modifications are discussed</li> </ul>
<p>Rationale:</p> <p>Relevant – Short of witnessing or participating in the approval process, reviewing a signed approval is the most direct form of supporting information available. Participation in sales meetings may also be relevant if such modifications are a standard discussion topic.</p> <p>Reliable – Reviewing signed approvals would generally be a reliable way to see that modifications were approved. Participation in sales meetings would only provide reliable information if <i>all</i> modifications are discussed. It would not provide information about modifications that were excluded from the discussion. Accordingly, such participation would not be reliable enough, on its own, to support a conclusion that all modifications are approved. However, participation in sales meetings might provide enough suitable information to influence the number, type and frequency of individual approvals the evaluator reviews.</p> <p>Note that objectivity may be a factor to consider. If the sales manager signs approvals and participates in the sales meetings, then the CFO may want a more objective, periodic evaluation.</p> <p>Timely – The timeliness of any approval review process will be dependent on the evaluator’s selection of contracts for review that are applicable to the period under consideration. The timeliness of participation in sales meetings is real-time and, thus, is timely.</p> <p>Sufficient – The organization’s conclusions regarding sufficiency could follow a thought process such as the following. The CFO’s participation in monthly sales meetings where modifications are discussed, coupled with a quarterly review by the controller (or testing by internal audit) of X number of contracts selected at random, would provide sufficient information to conclude whether the internal control system is effective in addressing this channel-stuffing risk (and possibly other contract-related risks).</p>	

Key Control	Available Information
Control #10 – Sales personnel compensation review & adjustment	<ul style="list-style-type: none"> <li>– CFO participation in the review/adjustment process</li> <li>– Completed and documented reviews/adjustments</li> </ul>
<p>Rationale:</p> <p>Relevant – Participation in this review and adjustment process provides the most relevant information about its completion. Seeing documented evidence of the reviews and adjustments provides the next most-relevant information.</p> <p>Reliable – Both forms of information above would reliably tell the evaluator whether this control was working. Again, objectivity could be a factor to consider.</p> <p>Timely – Similar to Control #6, timeliness depends on the evaluator selecting the right instances of the control to evaluate. Participation in the process is real-time and, thus, is timely.</p> <p>Sufficient – Deciding how much of this information to gather will follow a similar thought process as Control #6.</p>	
Control #11 – Sales and return trend review by salesperson, by customer	<ul style="list-style-type: none"> <li>– CFO participation in the review process</li> <li>– Completed and documented sales and return trend review</li> </ul>
<p>Rationale:</p> <p>The rationale for concluding on the persuasiveness of this information will be similar to the rationale for concluding on the information in Control #10.</p>	
Other Possibly Persuasive Information	Available Information
The organization might also determine how control failure might manifest in such a way as to be detected before material error can result. This may reveal other forms of indirect information that are useful in monitoring.	<ul style="list-style-type: none"> <li>– Revenue would increase, coupled with declining margins over time</li> <li>– Increase in accounts receivable aging on a per-sales-person basis</li> <li>– Increase in sales returns after quarter-end</li> </ul>
<p>Rationale:</p> <p>In this case, these potential risk indicators (i.e., indirect information) might be deemed to be relatively weak because they could take a long time to highlight a problem and are susceptible to being clouded by other business factors.</p>	

## Implement Monitoring Procedures

84. With risks prioritized, key controls selected and available persuasive information identified, the organization implements monitoring procedures that evaluate the internal control system's effectiveness. Monitoring involves the use of **ongoing monitoring** procedures and/or **separate evaluations** to gather and analyze persuasive information supporting conclusions about the effectiveness of internal control across all five COSO components.



### *Ongoing Monitoring and Separate Evaluations*

85. Ongoing monitoring procedures using both direct and indirect information are built into the routine, recurring operating activities of an organization. They include regular management and supervisory activities, peer comparisons and trend analysis using internal and external data, reconciliations, and other routine actions. They might also include automated tools that electronically evaluate controls and/or transactions. Because they are performed routinely, often on a real-time basis, ongoing monitoring procedures can offer the first opportunity to identify and correct control deficiencies.<sup>25</sup>

86. Separate evaluations can employ the same techniques as ongoing monitoring, but they are designed to evaluate controls *periodically* and are not ingrained in the routine operations of the organization.

87. Separate evaluations often are performed by people who are not directly involved in the operation of the controls being monitored. As such, they may provide a more objective analysis of control effectiveness than ongoing monitoring procedures that often are performed by less objective personnel.

<sup>25</sup> The COSO Framework states the following in Chapter 6. "Because [ongoing monitoring procedures] are performed on a real-time basis, reacting dynamically to changing conditions, and are ingrained in the entity, they are more effective than procedures performed in connection with separate evaluations. Since separate evaluations take place after the fact, problems will often be identified more quickly by the ongoing monitoring routines. Some entities with sound ongoing monitoring activities will nonetheless conduct a separate evaluation of their internal control system, or portions thereof, every few years. An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize 'building in' versus 'adding on' controls."

88. Separate evaluations can also provide valuable periodic feedback regarding the effectiveness of ongoing monitoring procedures.

89. Principle 19 of COSO’s 2006 Guidance,<sup>26</sup> which addresses the role of ongoing monitoring and separate evaluations, includes the following helpful attributes of monitoring:

- Integrates with operations — Ongoing monitoring is built into the organization’s routine operating activities.
- Provides objective assessments — Ongoing monitoring and/or separate evaluations provide an objective consideration of internal control effectiveness.<sup>27</sup>
- Uses knowledgeable personnel — Evaluators understand the components being evaluated and how those components relate to activities supporting the organization’s objectives.
- Considers feedback — Management and the board<sup>28</sup> receive feedback on the effectiveness of internal control.
- Adjusts scope and frequency — Management varies the scope and frequency of separate evaluations depending on the significance of risks being controlled, the nature of the controls mitigating those risks and the effectiveness of ongoing monitoring.

**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.”

“An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize ‘building in’ versus ‘adding on’ controls.”

“Usually, some combination of ongoing monitoring and separate evaluations will ensure that the internal control system maintains its effectiveness over time.”

<sup>26</sup> See Appendix A.

<sup>27</sup> COSO’s 2006 Guidance refers specifically to internal control over financial reporting, but these attributes are applicable to monitoring all COSO objectives.

<sup>28</sup> COSO’s 2006 Guidance states, “Management receives feedback on the effectiveness of internal control.” Although COSO’s 2006 Guidance does not specifically state that the board should receive feedback, the board’s need to receive such feedback is evident and is included here.



90. Most organizations employ a combination of ongoing monitoring and separate evaluations, with ongoing monitoring providing the primary support for management's day-to-day beliefs regarding control effectiveness, and separate evaluations providing periodic confirmation. This combination works best when the information used in the ongoing monitoring procedures is persuasive (as discussed below).

91. To determine how often separate evaluations will be performed, organizations consider the likelihood and/or potential significance of a control's failure between evaluations, including consideration of the support provided by ongoing monitoring. As the risk and/or significance of control failure increases/decreases, the interval between separate evaluations decreases/increases.

92. The level of persuasive information used in ongoing monitoring procedures can also influence the frequency of separate evaluations. Ongoing monitoring that evaluates more-persuasive information in a given risk scenario might provide all the support necessary to conclude on the effectiveness of the internal control system in that area. In such a case, separate evaluations might occur infrequently (perhaps even every few years<sup>29</sup>) and primarily for independent confirmation that the ongoing monitoring procedures are working.

93. Ongoing monitoring that evaluates less-persuasive information might flag anomalies that trigger an unscheduled separate evaluation, but generally would not provide the support necessary to conclude that internal control is effective over an extended period of time. Accordingly, more-frequent separate evaluations would be warranted.

---

<sup>29</sup> See the 1992 COSO Framework, page 70.

### Applying the Concepts – Implement Monitoring Procedures

The “Prioritize Risks” section discussed how the assessment of risk and the susceptibility of controls to failure work together to influence decisions regarding what controls to monitor. The information below extends that concept to this “Implement Monitoring Procedures” section of the guidance in order to show how those determinations might also affect the monitoring procedures employed and the information used in monitoring.

Monitoring Need	Determining Factors	Possible Monitoring Approach
Highest	Controls that: <ul style="list-style-type: none"> <li>– are susceptible to a high risk of failure, and</li> <li>– address risks deemed to be high-priority</li> </ul>	Ongoing monitoring using direct and indirect information, with periodic separate evaluations of direct information
Moderate in short term	Controls that: <ul style="list-style-type: none"> <li>– are less susceptible to failure, and</li> <li>– address risks deemed to be high-priority</li> </ul>	Ongoing monitoring using indirect information, with periodic separate evaluations of direct information
Moderate in long term	Controls that: <ul style="list-style-type: none"> <li>– are susceptible to a high risk of failure, and</li> <li>– address risks deemed to be lower-priority</li> </ul>	Ongoing monitoring using indirect information, with less-frequent separate evaluations of direct information
Lowest	Controls that: <ul style="list-style-type: none"> <li>– are less susceptible to failure, and</li> <li>– address risks deemed to be lower-priority</li> </ul>	Might not be monitored at all by senior management, or management may monitor them infrequently based on the level of risk.

Completing the earlier channel-stuffing example, the organization is now in position to determine what monitoring procedures to employ. Note that most of the procedures identified in the following table constitute ongoing monitoring that is already performed in the ordinary course of business. Additional monitoring procedures are added only to compensate for any remaining risk not covered by the normal operation of the internal control system.

4. Implement Monitoring Procedures	
Key Control	Monitoring Procedure
Control #1 – Tone at the top	<ul style="list-style-type: none"> <li>– The CFO participates in the monthly sales meeting, both establishing and verifying the proper tone at the top.</li> <li>– Internal audit also observes these meetings periodically.</li> </ul>
<p><b>Rationale:</b></p> <p>Participation in these meetings may be all that is necessary for the CFO to conclude on the effectiveness of this control. Evaluators who are further removed, such as the audit committee, might talk to the sales manager and/or sales personnel about management's attitudes and communications. This activity might be especially valuable if the organization does not have an internal audit function that can provide an objective assessment of control effectiveness.</p>	
Control #6 – Approval for contract modifications	<ul style="list-style-type: none"> <li>– Participation by CFO in monthly sales meetings.</li> <li>– Controller (or internal audit) to select X contracts every quarter, noting any unapproved modifications.</li> </ul>
<p><b>Rationale:</b></p> <p>Through weekly management meetings, the CFO may obtain valuable indirect information about the operation of this control. However, given the level of risk and the fact that sales personnel could make modifications that are not reported to the sales manager, the CFO might have the controller or internal audit randomly select a few contracts every quarter and review them for unapproved modifications.</p>	
Control #10 – Sales personnel compensation review & adjustment	<ul style="list-style-type: none"> <li>– CFO participation in this control is sufficient.</li> <li>– Audit committee to direct annual testing by internal audit.</li> </ul>
<p><b>Rationale:</b></p> <p>The CFO might review these adjustments and supporting documentation as part of his or her quarterly closing process, in which case, he or she has already performed the monitoring necessary to support related conclusions. The audit committee, as part of its oversight responsibility, might instruct internal audit to test this area annually. Alternatively, it might make direct inquiries regarding the compensation reviews and request proof of their completion.</p>	

Key Control	Monitoring Procedure
Control #11 – Sales and credit memo trend review	– Obtain evidence that the sales manager and CFO perform their review of sales spikes and credit memo spikes, including investigation of anomalies to determine the root cause and correction of any identified control deficiencies.
<p>Rationale:</p> <p>Since the CFO is involved in the completion of this control, he or she need not perform additional monitoring to reach a conclusion regarding its operating effectiveness. Like the previous step, the audit committee might direct internal audit to test this control when it tests the compensation review control, or audit committee members might perform their own inquiry and observation procedures.</p>	
Other Considerations	Monitoring Procedure
Additional periodic evaluation	– Every other year, internal audit selects a representative sample of contracts and tests for propriety.
<p>Rationale:</p> <p>The monitoring procedures above might reasonably be expected to evaluate, for an extended period, the effectiveness of the internal control system related to channel-stuffing risk. However, because the risk is high, and because it is most likely to occur through deceptive means, the organization could decide to have internal audit, or some other independent personnel, select and test samples of contracts and sales and return activities on an annual or bi-annual basis. These additional procedures would firmly establish the effectiveness of the controls and lend support to the belief that the other ongoing monitoring procedures are effective.</p>	

#### IV. Assess and Report Results

94. Monitoring includes reporting results to appropriate personnel. This final stage enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control or highlight identified deficiencies for possible corrective action. Principle 20 of COSO's 2006 Guidance ("Reporting Deficiencies") identified three helpful attributes that specifically address the role of monitoring when deficiencies are identified:<sup>30</sup>

- Report findings — Findings of internal control deficiencies 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 deficiencies — Significant deficiencies are communicated to top management and the board or audit committee.
- Correct problems on a timely basis — Deficiencies reported from both internal and external sources are considered, and timely corrective actions are taken.<sup>31</sup>

95. 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 assurance that the corrective action has been taken.

#### Prioritize and Communicate Results

96. Consistent with Principle 20 of COSO's 2006 Guidance, monitoring includes identifying potential control deficiencies and communicating them to the right people in a timely manner. Prioritizing identified control deficiencies can help facilitate the reporting process and the determination of possible corrective action. Some organizations prioritize 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). Other organizations use a less formal mechanism. Regardless, several factors may influence an organization's prioritization of identified deficiencies, including:

- The likelihood that the deficiency will affect the achievement of an organizational objective — The fact that a deficiency has been identified means that there is at least some likelihood that objectives may not be met. The greater that likelihood, the greater the severity of the control deficiency.

<sup>30</sup> See COSO's 2006 Guidance, page 94.

<sup>31</sup> See footnote 11 on page 8.

- The effectiveness of **compensating controls** — The effective operation of other controls may prevent or detect an error resulting from an identified deficiency before that error can materially affect the organization. The presence of such controls, when monitored, can provide support for reducing the severity of a deficiency.
- The aggregating effect of multiple deficiencies — When multiple deficiencies affect the same or similar risks, their mutual existence increases the likelihood that the internal control system may fail, thus increasing the severity of the identified deficiencies.

97. Determining who prioritizes the deficiencies is a matter of judgment. Organizations likely will consider the size and complexity of the organization, the nature and importance of the underlying risk, and the experience and authority of the people involved in the monitoring process. Regardless, the prioritization of identified deficiencies should be performed by appropriately competent and objective personnel.

#### Applying the Concepts — Prioritize and Communicate Results

The following table describes how organizations might consider the likelihood and significance variables as they prioritize identified control deficiencies. Smaller, less complex organizations might prioritize deficiencies in an informal manner through discussions within management and/or with the board. As organizations increase in size and complexity, they may need to formalize this process.

The assessment of the likelihood of a control failure and its potential significance are judgmental decisions that exist along a continuum. The table below is not meant to imply that there are four distinct categories of control failure. Rather, it is intended to demonstrate how one might distinguish between different risk grades.

Risk		Ranking Considerations
Significance	Likelihood	
High	High	<p>Highest priority – These control deficiencies deserve immediate attention. Additional oversight or review often can be implemented during the correction period to protect further against material errors.</p> <p>Example: a lack of experience or knowledge within an organization about accounting for a material, complex transaction.</p>

Risk		Ranking Considerations
Significance	Likelihood	
High	Low	<p>Moderate to high priority in the near term – The significance of the potential errors related to these control deficiencies makes the deficiencies important to correct. Additional oversight or review might also be implemented here during the correction period.</p> <p>Example: a weakness exists in the supervisory oversight of accounting for a complex, material transaction, but the experience and knowledge of the people responsible for the transaction are adequate. As such, the organization may conclude that the likelihood is low that an error will occur, but the significance is high if it does occur.</p>
Low	High	<p>Moderate priority in the long term – Potential errors resulting from these deficiencies can accumulate to material levels over time, or they can reduce organizational efficiency because frequent errors must be corrected repeatedly.</p> <p>Example: a weakness in a reconciliation control over an account that has low or moderate activity and for which large, single errors would be easily identified through the analysis of indirect information (e.g., metrics or key performance indicators). Weaknesses in such controls may grow over time, but are unlikely to result in an immediate material error, thus allowing the organization to prioritize their correction.</p>
Low	Low	<p>Lowest priority – The errors related to these control failures often result more in lost efficiency than in material errors. Management may consider these for correction, but not at the expense of failing to correct higher-ranking deficiencies.</p>

### Report Internally

98. Reporting protocols vary depending on the purpose for which the monitoring is conducted and the severity of the deficiencies. Typically, the results of monitoring conducted for purposes of evaluating internal control related to an organization's entity-wide 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 the organization's profitability.

99. Some monitoring, however, is conducted for purposes that might be relevant only to a part of an organization, e.g., a small subsidiary's operational monitoring to meet local goals that are not significant to the consolidated organization. Identified deficiencies in this case might have "higher likelihood" and "higher significance" relative to the subsidiary's objectives, but not to the organization's overall objectives. Reporting in such cases might be limited to local management personnel for whom the local goals are relevant.



100. In any case (except, perhaps, where fraud is suspected), control deficiencies should be reported to the person directly responsible for the control's operation and to management that has oversight responsibilities and is 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 and follow-up. At some point, deficiencies may become severe enough to warrant discussion with the board. Management and the board may wish to discuss in advance the nature and severity of deficiencies that should be reported to that level.

101. In situations where fraud is suspected, reporting may not occur to the person directly responsible for the control's operation. It would occur to higher levels, including to senior management and the board as appropriate.

### Applying the Concepts – Report Internally

Evaluators should understand what they should report and to whom concerning the results of their monitoring efforts. Depending on the size and complexity of the organization, this understanding may be established through formal or informal protocols. The potential significance of the underlying risk and the purpose for which the monitoring is being performed are often primary considerations in determining what to report and to whom.

The risk assessment process described in the “Prioritize Risks” section can help management and the board determine the risk areas in which they want to either (1) conduct monitoring procedures themselves (in which case, the internal reporting occurs automatically), or (2) receive periodic monitoring updates.

An internal audit function can also be a valuable resource both in identifying internal reporting needs and in delivering periodic reports regarding the results of monitoring procedures they perform.

As organizations grow in size and complexity, they may find value in using the process management tools referenced in the “Using Technology for Monitoring” section to document and track the results of internal control monitoring.

### Report Externally

102. A properly designed and executed monitoring program helps support external certifications or assertions<sup>32</sup> because it provides persuasive information that internal control operated effectively at a point in time or during a particular period.

<sup>32</sup> External assertions are statements (usually in writing) to external parties regarding the effectiveness of internal control. They may be required by regulation or contractual agreement. They may also be voluntary.

103. The presence of external assertion requirements may affect the type, timing and extent of monitoring an organization decides to perform. Therefore, organizations that are not required to report, and those that are required to report publicly or to third parties on the effectiveness of their internal control system, may design and execute monitoring activities differently.

104. External reports that assert as to the effectiveness of an internal control system may need to withstand scrutiny by outsiders who (1) do not have management's implicit knowledge of controls, and (2) require enough persuasive information to form their own opinions about the effectiveness of internal control. As a result, an organization may wish to compare the scope of its monitoring program with the needs of external parties, such as auditors and regulators, to help ensure that all parties understand the available monitoring information, enabling them to maximize its use. In addition, the organization might be able to enhance the efficiency of external parties' work by directing them to portions of its monitoring procedures that they might use, or by making modifications to its monitoring program to better facilitate external parties' work.

105. Most external reporting requirements are developed to address risks that are already contemplated by properly designed and executed monitoring procedures. They require assertions regarding the effectiveness of internal control systems in managing or mitigating risks that have a reasonable possibility of affecting certain organizational objectives. Effective monitoring procedures generally provide substantial support for such assertions. In some circumstances, however, modifications to the monitoring program may be warranted or beneficial to the organization when external reporting is required.

106. For example, when monitoring activities are performed by individuals who are objective, external parties (such as auditors and examiners) are likely to consider the results to be more reliable than those compiled by someone less objective. Organizations have choices regarding who conducts monitoring and should consider the cost of increasing the objectivity of the monitoring (e.g., by instituting a peer or supervisory review or directing internal audit to perform testing) compared with the cost of having the third party (such as an external auditor) develop its own reliable support. The most cost-effective option may be implementing a more objective monitoring process, thereby making the external party's work more efficient.

107. 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 external-party requirements such as an audit, regulatory examination or other third-party evaluation. For example, an organization's external auditors may determine, based on their audit plan, to evaluate the design and operating effectiveness of certain controls. If the organization uses *direct* information in monitoring those controls, independent auditors might use the results of that monitoring to provide support for their audit conclusions. Conversely, if the organization uses *indirect* information in

monitoring the controls, independent auditors may need to perform their own separate tests using direct information — possibly increasing the cost of the audit. Thus, when designing its monitoring procedures, the organization might consider the overall costs involved both in monitoring and in supporting any third-party evaluations.

### Applying the Concepts — Report Externally

External reporting requirements, such as for written assertions or confirmations regarding internal control effectiveness, sometimes lead management to conclude that separate evaluations (whose sole purpose is to support those requirements) must be implemented. However, management may be able to maximize the value of existing monitoring procedures by recognizing and/or modifying them for their ability to support management’s reporting requirements.

In considering the impact of external reporting requirements on monitoring, management and the board — possibly through discussion with their auditor or regulator — might consider the following:

- Do we fully understand the external reporting requirement, including its scope and expected level of documentation?
- Do reporting-requirement elements exist that might cause us to perform more-extensive monitoring in a particular area than we feel is necessary given our risk-assessment and control-importance analysis? If so, a review of the requirement (to help ensure that it does, in fact, require such an evaluation) and the risk assessment process (to help ensure that the organization did not omit an important risk and related control from normal monitoring consideration) may be in order. (Note that such conflicts should be rare, but may occur in some regulated environments.)
- Does the documentation adequately support the assertions?
- Could the organization make cost-effective modifications to the monitoring procedures that might improve the efficiency of third-party evaluations, such as the external audit (e.g., using more direct information, changing the timing or increasing the scope of evaluation so that the third party can use the results to support its conclusions)?
- Could the organization make cost-effective modifications to the format or extent of documentation that might improve the efficiency of third-party evaluations, such as the external audit or a regulatory exam?

## V. Other Considerations

### Monitoring Controls Outsourced to Others

108. When organizations use external parties (also known as service providers) to provide certain services, such as a bank outsourcing loan servicing or a corporation outsourcing its benefit plan administration, the associated risks to organizational objectives still must be managed properly. Users of outsourced services (often referred to as “user organizations”) should understand and prioritize the risks associated with those services. User organizations should also understand how the service provider’s internal control system manages or mitigates meaningful risks and obtain at least periodic information about the operation of those controls. This understanding may be attained through reviewing an independent audit or examination report provided by the service provider. Where such an audit or examination report is not available and where the level of risk warrants, user organizations may conduct their own periodic separate evaluations of key controls at the service provider. In fact, a “right to audit” clause is often included in contracts between user and service organizations.

109. User organizations may also find other useful sources of information about the design and operation of service organization controls such as through frequent interaction with the service provider, user group forums, and reports by internal auditors or regulatory authorities. Additionally, some user organizations may find it necessary to implement effective internal control over the processing performed by the service provider (e.g., comparison of input to output or reconciliation of service provider processing results to other independent records), which may reduce either the need to monitor controls of the service provider or the frequency with which to monitor them.

### Using Technology for Monitoring

110. Organizations often use information technology (IT) — via control monitoring tools and process management tools — to enhance monitoring. As the use of IT increases, both as part of an organization’s operations and as tools used in monitoring, the need increases to evaluate internal control over those information systems.<sup>33</sup>

---

<sup>33</sup> See Volume III, Chapter VI, for more detailed application techniques regarding the use of technology in monitoring.

111. *Control monitoring tools* — Automated control monitoring tools perform routine tests and can enhance 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 established 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. An example could include tools that monitor system access controls.
- Changes — Identifying and reporting changes to critical resources, data or information, making it possible to verify 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, error logs or exception reports, typically as part of an application system.

112. Some control monitoring tools are used to perform what is often referred to as “continuous controls monitoring.” These tools complement normal transaction processing by checking every transaction, or selected transactions, for the presence of certain anomalies (e.g., identifying transactions that exceed certain thresholds, analyzing data against predefined criteria to detect potential controls issues such as duplicate payments, or electronically identifying segregation of duties issues). Many of these tools serve more as highly effective control activities (detecting individual errors and targeting them for correction before they become material) than they do as internal control monitoring activities. Regardless, if they operate with enough precision to detect an error before it becomes material, they can enhance the efficiency and effectiveness of the whole internal control system and may be key controls whose operation should be monitored.

113. To the extent that manual procedures, such as review and follow-up, are necessary components of these tools, their effectiveness should be considered.

114. *Process management tools* — Process management tools are designed to make monitoring more efficient and sustainable by facilitating some of the activities that affect monitoring 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 and reporting 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 deficiencies, including their severity and any remediation activities;
- Support the “roll-up” of information about risks and controls at various levels 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.

### Formality and Level of Documentation

115. Management and boards of smaller organizations may need less documentation to support conclusions regarding control effectiveness — especially where senior management and the board have direct knowledge of the internal control system’s operation. As organizations increase in size, the level of direct knowledge declines at the senior-management and board levels, thus increasing the need for more-formal monitoring documentation.

116. When external reporting is required (especially reporting that is subject to examination by auditors, regulators or other external parties), organizations of all sizes may find that more-formal documentation is a cost-effective way to improve the efficiency of meeting those requirements. For example, an external auditor, regulator or other external party may be able to conduct a more efficient audit or examination if he or she has access to documentation that demonstrates the results of management’s monitoring.

117. More-formal documentation can be achieved through manual processes or through the use of software tools designed to retain and report the results of monitoring.

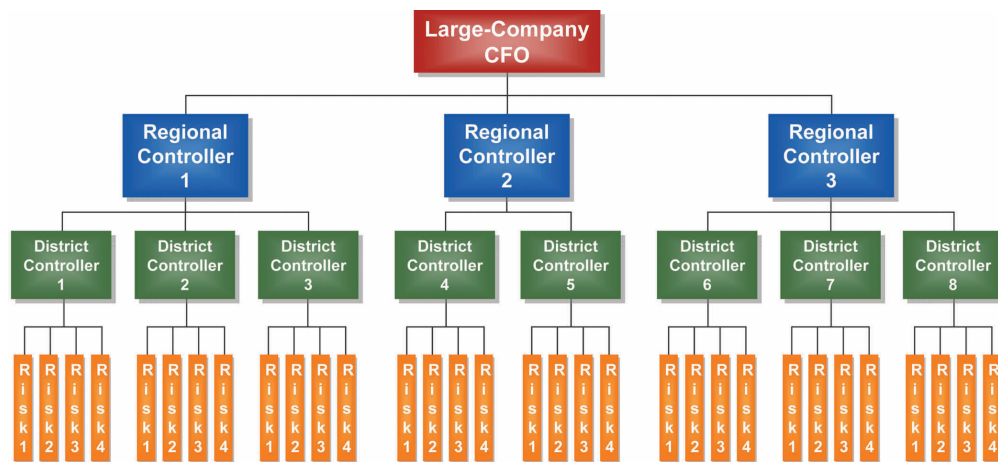
118. Beyond adjusting the formality and level of documentation, organizations may find benefit and cost-effectiveness in coordinating certain monitoring procedures with any external parties who may conduct an independent audit or examination of internal control.

### Scalability of Monitoring

119. Many factors can influence the type, timing and extent of an organization’s monitoring. Two factors that warrant special mention are organizational size and complexity, both of which have been discussed throughout this guidance. Following are some additional thoughts regarding the impact of size and complexity.

#### Scalability Based on Size

120. Organizational size affects the design and conduct of monitoring. In most large organizations, neither senior management nor the board is in close proximity to the operation of many controls. As a result, they often rely on monitoring procedures performed by other personnel through successive levels of management. These procedures are built into the day-to-day, ongoing monitoring activities that operate at each level of the organization (Figure 9<sup>34</sup>), all of which “roll up” to a home office or headquarters, and typically are augmented by separate 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.



Sample Large-Company Financial Reporting Monitoring Structure  
**Figure 9**

<sup>34</sup> Note: this example and the example in Figure 10 are designed to demonstrate a hypothetical monitoring structure covering risks that fall within the CFO’s area of responsibility. They are illustrative and are not meant to imply that the CFO is at the head of every monitoring program or that risk exists only at the lowest levels of an organization.



121. In smaller organizations, on the other hand, monitoring at the senior-management level often occurs much closer to the risk and related controls, giving the evaluators more direct information about the operation of controls. Monitoring in the smaller organization (Figure 10) can look much like monitoring at lower levels



Sample Small-Company Financial Reporting Monitoring Structure  
**Figure 10**

in a large organization (Figure 9). The primary difference is that the lead evaluator (the CFO in the examples) in the larger organization performs more monitoring of other monitoring procedures, where the lead evaluator in the smaller organization performs more monitoring of actual internal controls. The greater quantity of direct information about the operation of internal control may allow the evaluator in a smaller organization to support his or her control conclusions without adding the additional monitoring procedures that may be necessary in a larger organization where the evaluator is further removed from the operation of controls.

122. Large organizations do have the advantage of scale. Because their risks are more dispersed, control problems that are confined to one area may not be material to the organization as a whole. 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, an organization that has only one person processing invoices cannot afford for that person to be improperly trained; such a deficiency would increase the importance of management's daily observation of internal control. 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, placing greater importance on the monitoring activities of the board or audit committee.

123. Small organizations, however, can be more efficient than large organizations in prioritizing risks, identifying controls for evaluation and determining what information to use in the evaluation process because knowledge about risks and controls typically is contained within a small group.

### *Scalability Based on Complexity*

124. 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 certain types of transactions (e.g., complex capital structures, derivative transactions or acquisitions).

125. 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. For example, an organization may use a prepackaged information system for one of its business processes, which can reduce certain IT-related risks (such as the risk of incorrect programming), but that same organization might also use a complex internally developed software system for another business process which, unless well-controlled, can increase IT-related risks.

126. The level of complexity generally correlates with the level of risk. Accordingly, in areas of greater organizational complexity, one might expect more ongoing monitoring using direct information. In contrast, in areas of lesser complexity, ongoing monitoring using indirect information, along with periodic confirmation through separate evaluations that use direct information, might be appropriate.

127. Clearly, any plan for monitoring — if it is to remain effective and efficient — must recognize the variables that affect monitoring and be able to adapt to them as necessary. This implies that monitoring is not one-size-fits-all, but is unique to each organization's risk profile and internal control structure.

## VI. Assessing the Effectiveness and Efficiency of Monitoring

128. 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.

129. As the COSO Framework indicates, the monitoring component of internal control “ensures that internal control continues to operate effectively.”<sup>35</sup> The ultimate goal of monitoring is met when organizations use the most efficient means possible to gather and evaluate appropriately persuasive information about the effectiveness of the internal control system in addressing meaningful risks to organizational objectives. Accordingly, it may be helpful to periodically evaluate the overall effectiveness and efficiency of monitoring. The following questions — which may be asked at various levels, including the board level — may help in that regard.

### Effectiveness

1. Has the organization appropriately considered all of the risks that could materially affect its objectives?
2. What recent changes have taken place within the organization’s environment, people, processes or technology, and did the organization properly consider the impact of those changes on internal controls, including possible alteration of related monitoring procedures?
3. How long has it been since the organization discussed, at an appropriate level of detail, the risks the organization faces related to operations, financial reporting, or compliance with laws and regulations? Is that period of time acceptable?
4. Have errors resulted from control failures that were not detected on a timely basis by the organization’s routine monitoring procedures? If so, what changes in monitoring could prevent similar control failures?
5. What do the results of internal audits, external audits or regulatory exams tell the organization about the effectiveness of monitoring?
6. Does the organization have a process for tracking control deficiencies through evaluation and remediation?
7. Have all identified deficiencies been addressed properly?

<sup>35</sup> COSO Framework, p. 69.

### Efficiency

1. Is the organization monitoring controls at a cost, effort or organizational level that is inconsistent with the amount of risk the controls mitigate?
2. Is the organization monitoring internal controls in areas that have never had a control failure and have not been known to cause errors in similar organizations? (Note: this may not be a reason to omit monitoring procedures, but it may affect the desired type, timing and extent of monitoring, including at what organizational level monitoring might be performed.)
3. Do risk areas exist within the organization that rarely experience meaningful change and which, given their level of risk, might lend themselves to control monitoring that varies in scope over time (e.g., using indirect information over longer periods of time between control baselines established using direct information)?
4. Does unwarranted duplication of effort occur where multiple people monitor the effectiveness of the same controls and where, given the level of risk, redundancy is not necessary?
5. Does the organization conduct additional evaluation procedures implemented solely to meet regulatory or other requirements? If so, are there elements of the organization's normal monitoring procedures that might provide the necessary level of monitoring support?



## 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. Although developed specifically for smaller companies to consider in evaluating internal control over financial reporting, these principles can be useful to all organizations regardless of size and for internal control objectives beyond those associated with financial reporting. 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 Deficiencies — Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.




## Map Linking the Model for Monitoring to the 1992 COSO Framework


The table below demonstrates how the model for monitoring presented on page 7 links to, and is derived from, the 1992 COSO Framework.

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
 <b>Establish a Foundation</b>		
<b>Tone at the top</b>	17	<p>The control environment provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components. <i>Within this environment</i>, management assesses risks to the achievement of specified objectives. Control activities are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant information is captured and communicated throughout the organization. <i>The entire process is monitored and modified as conditions warrant.</i> [Emphasis added]</p>
	23	<p>The control environment sets the tone of an organization, influencing the control consciousness of its people. <i>It is the foundation for all other components of internal control, providing discipline and structure.</i> Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors. [Emphasis added]</p>
	23	<p>The control environment has a pervasive influence on the way business activities are structured, objectives established and risks assessed. <i>It also influences control activities, information and communication systems, and monitoring activities.</i> This is true not only of their design, but also the way they work day to day. The control environment is influenced by the entity's history and culture. It influences the control consciousness of its people. <i>Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive "tone at the top."</i> They establish appropriate policies and procedures, often including a written code of conduct, which foster shared values and teamwork in pursuit of the entity's objectives. [Emphasis added]</p>

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
	23	The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer and monitor them. <i>Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of other internal control components.</i> [Emphasis added]
<b>Organizational structure</b>	27	An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored.
	26–27	<p>The control environment and "tone at the top" are influenced significantly by the entity's board of directors and audit committee. Factors include the board or audit committee's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and the appropriateness of its actions. Another factor is the degree to which difficult questions are raised and pursued with management regarding plans or performance. Interaction of the board or audit committee with internal and external auditors is another factor affecting the control environment.</p> <p>Because of its importance, an active and involved board of directors, board of trustees or comparable body — possessing an appropriate degree of management, technical and other expertise coupled with the necessary stature and mind set so that it can adequately perform the necessary governance, guidance and oversight responsibilities — is critical to effective internal control. And, because a board must be prepared to question and scrutinize management's activities, present alternative views and have the courage to act in the face of obvious wrongdoing, it is necessary that the board contain outside directors. Certainly, officers and employees often are highly effective and important board members, bringing knowledge of the company to the table. But there must be a balance. Although small and even mid-size companies may find it difficult to attract or incur the cost of having a majority of outside directors — usually not the case with large organizations — it is important that the board contain at least a critical mass of outside directors. The number should suit the entity's circumstances, but more than one outside director normally would be needed for a board to have the requisite balance.</p>
	69	This process involves assessment by <i>appropriate personnel</i> of the design and operation of controls on a suitably timely basis, and the taking of necessary actions. [Emphasis added]

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
	86–87	<p>The audit committee (or the board itself, where no audit committee exists) is in a unique position: It has the authority to question top management regarding how it is carrying out its financial reporting responsibilities, and it also has authority to ensure that corrective action is taken. The audit committee, in conjunction with or in addition to a strong internal audit function, is often in the best position within an entity to identify and act in instances where top management overrides internal controls or otherwise seeks to misrepresent reported financial results. Thus, there are instances where an audit committee, or board, must carry its oversight role to the point of directly addressing serious events or conditions.</p>
<b>Baseline understanding of internal control effectiveness</b>	69	<p>Internal control systems change over time. The way controls are applied may evolve. Once-effective procedures can become less effective or perhaps are no longer performed. This can be due to the arrival of new personnel, the varying effectiveness of training and supervision, time and resource constraints or additional pressures. Furthermore, circumstances for which the internal control system originally was designed also may change, causing it to be less able to warn of the risks brought by new conditions. Accordingly, management needs to determine whether the internal control system continues to be relevant and able to address new risks.</p>
	72	<p>The evaluator must understand each of the entity activities and each of the components of the internal control system being addressed. It may be useful to focus first on how the system purportedly functions, sometimes referred to as the system design. This may involve discussions with entity personnel and review of existing documentation.</p> <p>The evaluator must determine how the system actually works. Procedures designed to operate in a particular way may over time be modified to operate differently. Or, they may no longer be performed. Sometimes new controls are established but are not known to persons who described the system and are not included in available documentation. A determination as to the actual functioning of the system can be accomplished by holding discussions with personnel who perform or are affected by controls, by examining records on performance of the controls or a combination of procedures.</p> <p>The evaluator must analyze the internal control system design and the results of tests performed. The analysis should be conducted against the backdrop of the established criteria, with the ultimate goal of determining whether the system provides reasonable assurance with respect to the stated objectives.</p>

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
 <b>Design &amp; Execute</b>		
<b>Prioritize risks</b>	71	<p>Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most critical to reducing a given risk will tend to be evaluated more often. Evaluation of an entire internal control system — which will generally be needed less frequently than the assessment of specific controls — may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. When a decision is made to evaluate an entity's entire internal control system, attention should be directed to each of the internal control components with respect to all significant activities. The evaluation scope will also depend on which of the three objectives categories — operations, financial reporting and compliance — are to be addressed. [Emphasis added]</p>
<b>Identify controls</b>	71	See the quote above
<b>Identify persuasive information about controls</b>	70–71	Each of the examples of ongoing monitoring on pages 70–71 demonstrate how various forms of direct and indirect information can be evaluated through ongoing monitoring procedures.
	71	While ongoing monitoring procedures usually provide important feedback on the effectiveness of other control components, it may be useful to take a fresh look from time to time, focusing directly on the system's effectiveness. This also provides an opportunity to consider the continued effectiveness of the ongoing monitoring procedures.
<b>Implement monitoring procedures</b>	69–70	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. 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. In making that determination, consideration should be given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
		that the internal control system maintains its effectiveness over time.
		It should be recognized that ongoing monitoring procedures are built in to the normal, recurring operating activities of an entity. Because they are performed on a real-time basis, reacting dynamically to changing conditions, and are ingrained in the entity, they are more effective than procedures performed in connection with separate evaluations. Since separate evaluations take place after the fact, problems will often be identified more quickly by the ongoing monitoring routines. Some entities with sound ongoing monitoring activities will nonetheless conduct a separate evaluation of their internal control system, or portions thereof, every few years. An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize “building in” versus “adding on” controls.
 <b>Assess &amp; Report</b>		
<b>Prioritize findings</b>	75	In considering what needs to be communicated, it is necessary to look at the implications of findings.
<b>Report results to appropriate level</b>	69	Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.
	75	Certainly, all internal control deficiencies that can affect the entity’s attaining its objectives should be reported to those who can take necessary action, as discussed in the next section. The nature of matters to be communicated will vary depending on individuals’ authority to deal with circumstances that arise and the oversight activities of superiors.
	75	It can be argued that no problem is so insignificant as to make investigation of its control implications unwarranted. An employee’s taking of a few dollars from a petty cash fund for personal use, for example, would not be significant in terms of that particular event, and probably not in terms of the amount of the entire petty cash fund. Thus, investigating it might not be worthwhile. However, such apparent condoning of personal use of the entity’s money might send an unintended message to employees.
	75	Information generated by employees in conducting regular operating activities usually is reported through normal channels to their immediate superior. He or she may in turn communicate upstream or laterally in the organization so that the information ends up with people who can and should act on it. As discussed in Chapter 5, there should be alternative

2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
		<p>communications channels for reporting sensitive information such as illegal or improper acts.</p> <p>Findings of internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.</p>
	76	<p>Providing needed information on internal control deficiencies to the right party is critical to the continued effectiveness of an internal control system. Protocols can be established to identify what information is needed at a particular level for decision-making.</p> <p>Such protocols are based on the general rule that a manager should receive control information needed to affect action or behavior of people under his or her responsibility, or to achieve the activity's objectives. A chief executive normally would want to be apprised, for example, of <i>very serious infractions</i> of policies and procedures. He or she would also want supporting information on the nature of <i>matters that could have significant financial consequences or strategic implications</i>, or that could affect the entity's reputation. Senior managers should be apprised of control deficiencies affecting their units. Examples include where assets with a specified monetary value are at risk, where the competence of personnel is lacking or where important financial reconciliations are not performed correctly. Managers should be informed of control deficiencies in their units in increasing levels of detail as one moves down the organizational structure.</p> <p><i>Protocols are established by supervisors, who define for subordinates what matters should be reported.</i> The degree of specificity will vary, usually increasing at lower levels in the organization. While reporting protocols can inhibit effective reporting if too narrowly defined, they can enhance the reporting process if sufficient flexibility is provided.</p> <p>Parties to whom deficiencies are to be communicated sometimes provide specific directives regarding information to be reported. A <i>board of directors or audit committee, for example, may ask management or internal or external auditors to communicate only those findings of deficiencies meeting a specified threshold of seriousness or importance.</i> One such threshold used by the public accounting profession is "reportable conditions." They are defined as: ... significant</p>



2008 Guidance Model for Monitoring	1992 Pg. No.	1992 COSO Framework Text
		<p>deficiencies in the design or operation of the internal control structure, which could adversely affect the organization's ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements.</p> <p>This definition relates to financial reporting objectives, though the concept probably could be adapted to cover operations and compliance objectives as well. [Emphasis added]</p>
<b>Follow up on corrective action</b>	75	<p>Findings of internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, <i>who is in the position to take corrective action</i>, but also to at least one level of management above the directly responsible person. <i>This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.</i> [Emphasis added]</p>
	77	<p>Personnel in a smaller entity usually have a clear understanding of the types of problems that need to be reported upstream. <i>What may not always be apparent is who is responsible for determining the cause of a problem and taking corrective action. This is as important to a small or mid-size organization as it is for a large one.</i> [Emphasis added]</p>



## Glossary

Accuracy or accurate	In monitoring, accuracy is the degree to which information can reasonably be expected to be free from error and/or to communicate results that reflect reality.
Change management	Relative to monitoring, change management is the act of verifying that (1) necessary changes in the design or operation of internal control are made, and (2) when changes are made, they are made correctly. The goal is to render the internal control system capable of providing reasonable assurance that organizational objectives will be achieved.
Compensating controls	Compensating controls serve to accomplish the objective of another control that did not function properly, thus helping to reduce risk to an acceptable level.
Competence or competent	Competence refers to the evaluator's knowledge of the controls and related processes, including how controls should operate and what constitutes a control deficiency.
Control activities	Control activities are the policies and procedures that help ensure that management directives are carried out and 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 designed and implemented to achieve the organization's internal control objectives. A control baseline serves as an appropriate starting point for effective control monitoring.



Control environment	<p>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:</p> <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	<p>Relative to monitoring, control objectives provide specific targets against which to evaluate the effectiveness of internal control. 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.</p>
Deficiency or internal control deficiency	<p>A condition within an internal control system worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the internal control system to provide a greater likelihood that the entity's objectives will be achieved.</p>
Direct information	<p>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 effective operation of controls.</p>



Evaluator	<p>Evaluators are individuals who are responsible for monitoring internal control at various levels throughout an organization. Effective internal control systems include evaluators who have appropriate capabilities, objectivity, authority and resources that enable them to (1) understand the risks that can materially affect the organization’s objectives, (2) identify the controls that are critical to managing or mitigating those risks, and (3) conduct and/or oversee the monitoring of appropriately persuasive information about the effectiveness of the internal control system. Evaluators often include management and line-personnel, as well as internal auditors. Board members also serve as evaluators when they monitor the activities and conduct of senior management. The two primary attributes of effective evaluators are competence and objectivity.</p>
Indirect information	<p>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 it can identify anomalies that are indicative of a potential control failure.</p> <p>When evaluators begin with a baseline understanding of internal control effectiveness, established through the use of persuasive direct information, the evaluation of indirect information can be a valuable monitoring tool that may:</p> <ul style="list-style-type: none"><li>• Signal that a change in the environment or control operation has occurred, or</li><li>• Supplement the support provided by direct information — sometimes for an extended time frame — regarding the evaluator’s conclusions about control effectiveness.</li></ul> <p>As a result, monitoring using indirect information can influence the type, timing and extent of future monitoring procedures that use direct information.</p>
Internal control	<p>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.</p>



Key controls	<p>Key controls are those that, when evaluated, provide support for a reasonable conclusion about the entire internal control system's ability to achieve the underlying objectives. They may operate within any or all of COSO's five components.</p> <p>Key controls often have one or both of the following characteristics:</p> <ul style="list-style-type: none"> <li>• Their failure could materially affect the objectives for which the evaluator is responsible, but might not be detected in a timely manner by other controls, and/or</li> <li>• Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization's objectives.</li> </ul>
Key performance indicators	<p>Key performance indicators are metrics that reflect critical success factors. They help organizations measure progress towards goals and objectives.</p>
Key risk indicators	<p>Key risk indicators are forward-looking metrics that seek to identify potential problems, thus enabling an organization to take timely action, if necessary.</p>
Material or materially	<p>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>).</p>
Meaningful risks	<p>Meaningful risks are those that, in a given time frame, might reasonably have a consequential effect on an organizational objective.</p>
Objective (adj.) or objectivity	<p>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.</p>



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 guidance, 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 at appropriate levels in the organization. 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.
Self-assessment	Self-assessment occurs when persons responsible for a particular unit or function determine the effectiveness of controls for their activities. The term is often used to describe assessments made by the personnel who operate the control (i.e., self-review). It can also describe more-objective personnel who are not responsible for operating the control. In this guidance those “other, more objective personnel” would include persons performing peer or supervisory review.
Self-review	In this guidance the term “self-review” refers narrowly to the review of one’s own work. It represents the least objective type of “self assessment” described above.
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 deficiencies before they become material to an organization.
Verifiable or verifiability	Verifiable information is information that can be established, confirmed or substantiated as true or accurate.

