Internal Control —
Integrated Framework

Guidance on Monitoring
Internal Control Systems

Volume II — Guidance

June 2008

Exposure Draft
Public Comment Period
Closes August 15, 2008
Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Larry E. Rittenberg  
COSO Chair

Mark S. Beasley  
American Accounting Association

Charles E. Landes  
American Institute of Certified Public Accountants

Edith G. Orenstein  
Financial Executives International

Michael P. Cangemi  
Financial Executives International

David A. Richards  
The Institute of Internal Auditors

Jeffrey Thomson  
Institute of Management Accountants

Grant Thornton LLP — Author

Principal Contributors

R. Trent Gazzaway (Project Leader)  
Managing Partner of Corporate Governance  
Grant Thornton LLP — Charlotte

James P. Burton  
Partner  
Grant Thornton LLP — Denver

J. Russell Gates  
President  
Dupage Consulting LLC — Chicago

Keith O. Newton  
Partner  
Grant Thornton LLP — Chicago

Sridhar Ramamoorti  
Partner  
Grant Thornton LLP — Chicago

Richard L. Wood  
Partner  
Grant Thornton LLP — Toronto

R. Jay Brietz  
Senior Manager  
Grant Thornton LLP — Charlotte

Review Team

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

Dorsey L. Baskin Jr.  
Regional Partner of Professional Standards  
Grant Thornton LLP — Dallas

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

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

COSO Task Force

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

Douglas J. Anderson  
Corporate Auditor  
Dow Chemical Company

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

Richard D. Brounstein  
Chief Financial Officer, NewCardio, Inc.  
Director, The CFO Network

Jennifer M. Burns  
Partner  
Deloitte & Touche LLP

Paul Caban  
Assistant Director  
U.S. Government Accountability Office

James W. DeLoach  
Managing Director  
Protiviti

Miles E. Everson  
Partner  
PricewaterhouseCoopers LLP

Audrey A. Gramling  
Associate Professor  
Kennesaw State University

Scott L. Mitchell  
Chairman and CTO  
Open Compliance & Ethics Group

James E. Newton  
Partner  
KPMG LLP

John H. Rife  
Partner  
Ernst & Young LLP

Michael P. Rose  
CEO and Senior Partner  
GR Consulting LLP

Robert S. Roussey  
Professor of Accounting  
University of Southern California

Andre Van Hoek  
Vice President, Corporate Controller  
Celgene Corporation

Observers

Securities and Exchange Commission

Josh K. Jones  
SEC Observer  
Professional Accounting Fellow
# COSO Guidance on Monitoring

## Table of Contents

### I. Monitoring as a Component of Internal Control Systems
- Role of Monitoring 2
- Structure of Effective Internal Control Systems 5
- A Model for Monitoring 7

### II. Establishing a Foundation for Monitoring
- Tone from the Top 8
- Organizational Structure 9
- Baseline Understanding of Internal Control Effectiveness 13

### III. Designing and Executing Monitoring Procedures
- Understand and Prioritize Risks 19
- Understand the Internal Control System and Identify Key Controls 22
- Identify Persuasive Information 27
- Implement Monitoring Procedures 38

### IV. Assessing and Reporting Results
- Prioritizing and Communicating Results 45
- Reporting Internally 47
- Reporting Externally 48

### V. Scalability of Monitoring
- Scalability Based on Size 50
- Scalability Based on Complexity 51
- Formality of Monitoring and Level of Documentation 52

### VI. Assessing the Effectiveness and Efficiency of Monitoring 53

**Appendix:** Principles of Effective Internal Control Over Financial Reporting A-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.”

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 helpful to all organizations, regardless of size. Its 20 principles (see 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 should be designed and implemented to provide information on whether the internal control system operates effectively over time, and (2) 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.

---

1 COSO Framework, p. 69.
2 See COSO’s 2006 Guidance, Frequently Asked Questions Volume, Question #17.
3 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. 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, internal control evaluation procedures designed to test 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 forced them to implement inefficient year-end evaluations to support their conclusions as of the end of the fiscal year.

4. This Guidance on Monitoring Internal Control Systems (COSO’s Monitoring Guidance) is intended to help any organization design, implement, and evaluate monitoring procedures that achieve the principles of the monitoring component in an 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\(^4\) regarding the achievement of the organization’s objectives.\(^5\) 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 — which includes all five components — continues to operate effectively over time. Thus, it provides valuable evidence to support 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 way the internal control system addresses meaningful risks.

- 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.

7. Monitoring leads to the identification and correction\(^6\) of control deficiencies before they materially affect the achievement of the organization’s objectives. Using the financial reporting objective as an example, monitoring should identify and correct control deficiencies before the failure of the underlying controls leads to a material misstatement of an organization’s published financial statements. For the operations objective, monitoring should identify and correct deficiencies in controls over a manufacturing process before they lead to the production and sale of defective products.

---

\(^4\) Many organizations have boards of directors and related board committees to help oversee the conduct of their activities. Other organizations may not have a formal board of directors, but may have other stakeholders who serve in a governance and oversight capacity. For simplicity, this guidance will use the terms “board of directors” or “board” to refer to all groups charged with governance and management oversight.

\(^5\) COSO Framework, p. 15.

\(^6\) The activity of correcting deficiencies may also be classified in the risk assessment or control activities component. 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.
8. Properly designed and executed monitoring helps ensure and promote good internal control operation. It requires thoughtful planning that leads to the evaluation of **persuasive information**, which is both **suitable** and **sufficient** in the circumstances.\(^7\)

9. In contrast, ineffective monitoring, over time, allows the natural deterioration of internal control systems. Absent effective monitoring, controls within any or all of the five components may change, cease to operate, or lose effectiveness because of changes in circumstances. Monitoring should be designed to detect such changes in a timely fashion.

10. No system of internal control can guarantee the prevention and detection of all control deficiencies that result in the inability to achieve organizational objectives. However, when properly designed and executed, monitoring will help ensure that internal control continues to operate effectively. Monitoring is most effective and efficient when it considers how the *entire* internal control system manages the risks to achieving the organization’s objectives. In contrast, it is less effective and efficient when it focuses on a checklist of control activities\(^8\) that are selected for evaluation without regard to (1) the level of the risk they address, or (2) their relative importance in addressing the risk.

11. Most organizations will find that many elements of monitoring described in this guidance are part of their normal 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.

---

7 See the discussion of persuasive information beginning on page 27.

8 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.
Structure of Effective Internal Control Systems

12. 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.\(^9\)

13. 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.

14. The concepts embodied in the COSO Framework are frequently presented in terms of a three-dimensional cube (see page 1, Figure 1) that depicts the five components operating across each internal control objective\(^10\) and within all organizational units and activities.

15. 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 from 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.

16. 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 ability, in its entirety, to manage or mitigate meaningful risks to organizational objectives.

---

10 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.
Monitoring does *not* seek to conclude on the effectiveness of individual internal control components operating in isolation.

17. This process view of the COSO Framework also shows that internal controls\(^\text{11}\) 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).

18. 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 can be designed or adjusted *after* other elements of the internal control system have been implemented.

\(^{11}\) See footnote 8 on page 4.
A Model for Monitoring

19. Management implements monitoring by (see Figure 3):

1. Establishing a foundation for monitoring, including:
   - A tone from 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, and authority in monitoring roles, and
   - A baseline understanding of internal control effectiveness.

2. Designing and executing monitoring procedures that:
   - Are prioritized based on the importance of the control to achievement of the objective (i.e., the risk associated with the control’s failure), and
   - Gather and evaluate information that is persuasive in terms of its ability to tell evaluators whether the internal control system is operating effectively.
3. Assesing and reporting results in order to:
   - Prioritize findings,
   - Provide support for conclusions regarding the effectiveness of internal control, and
   - Facilitate prompt corrective actions where necessary.

II. Establishing a Foundation for Monitoring

20. Planning and organizational support form the foundation for monitoring, which includes (1) a tone from 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, and authority, and (3) a baseline understanding of internal control effectiveness.

Tone from the Top

21. 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

Expressing a positive tone from 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 that are important to managing or mitigating those risks. Expectations can be emphasized in periodic meetings or in performance reviews, or may be written into job descriptions. As organizations grow in size, these communications may need to be more formalized.

---

12 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.
• 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.

**Organizational Structure**

22. Monitoring operates most effectively when (1) the roles and responsibilities of management and the board regarding monitoring are appropriate and clearly articulated, and (2) evaluators with proper characteristics are placed in the right positions.

**Role of Management and the Board**

23. As noted earlier, management has the primary responsibility for the effectiveness of an organization’s internal control system. Management establishes the system and makes sure that it continues to operate effectively. Controls performed below the senior-management level can be monitored by management personnel or their objective designees. However, controls performed directly by members of senior management cannot be monitored objectively by those individuals or their designees. In such circumstances, other members of senior management may be able to monitor the controls. For example, the chief legal officer might monitor controls over new corporate contracts entered into by the chief operating officer. The board may also need to monitor such controls, which it frequently accomplishes through an audit committee and an internal audit function. Board-level monitoring becomes increasingly important regarding controls that are at risk of senior-management override.

24. In most cases, the board is ultimately responsible for determining whether management has implemented effective internal control (including monitoring). It makes this assessment by (1) understanding the risks the organization faces, and (2) gaining an understanding of how senior management manages or mitigates those risks that are meaningful to the organization’s objectives. Obtaining this understanding includes determining how management supports its beliefs about the effectiveness of the internal control system in those important areas.
Applying the Concepts

In most organizations, 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.

In small organizations, the board may not have access to an internal audit function. The absence of this resource increases the need for board members to interact with non-management personnel and possibly creates the need to observe some controls in operation, especially controls in areas of higher risk. As organizations grow in size and complexity, the board may need to hire or engage internal auditors or other experts to help evaluate the effectiveness of the internal control system in certain areas.

If the external auditor’s work identifies 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, neither management nor the board should plan to reduce its monitoring efforts in other areas simply because the external auditor did not find errors or control deficiencies.

Characteristics of Evaluators

25. 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 various areas of the organization who, as part of their normal 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, knowledge and authority, as well as an understanding of the risks that the controls are intended to manage.

26. 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.
27. Some people who are involved in the monitoring process — although they do not have the responsibility for designing monitoring procedures or for reaching final conclusions regarding control effectiveness — do produce information the evaluators use to reach their final conclusions. For example, a divisional controller may have certain monitoring procedures dictated from the home office or may provide information that is used by a regional manager to perform the monitoring function. These personnel are vital to 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.

28. **Competence** and **objectivity** considerations help organizations determine who should perform monitoring procedures. Competence refers to the evaluator’s knowledge of the controls and related processes, including how controls should operate and what constitutes a control deficiency. As noted earlier, monitoring requires both 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 will be useful in that regard.

29. The evaluator’s objectivity refers to the extent to which he or she can be expected to perform an evaluation with no concern about possible personal consequences and no vested interest in manipulating the information 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 affected by the results of monitoring. Later, in the “Suitable Information” section, this guidance extends the discussion of objectivity to the information sources that evaluators use when they perform monitoring.
30. The evaluator’s objectivity can be viewed along a continuum from least to most objective (see Figure 5). **Self-review**\(^{13}\) (the evaluation of one’s own work) is least objective and, thus, is limited in its ability to support conclusions about the effectiveness of important 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.

31. **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.

32. 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.

33. On a relative basis, senior management in smaller 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 smaller 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.

---

\(^{13}\) 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.
Applying the Concepts

Management might consider a two-step process to place people with the right skills and objectivity 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.

Once monitoring leadership is established, it can match the skills and objectivity needed by evaluators with the relative importance of 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 to perform monitoring procedures in certain areas or directing independent board members with appropriate expertise to perform monitoring activities.

Baseline Understanding of Internal Control Effectiveness

34. Changes in the external environment or in the manner in which internal control systems operate create risks to the organization’s objectives that the internal control system may fail to manage. Regulatory changes, changes in customer demands, and new product lines are examples of events in the environment that could create new risks to the achievement of objectives if the internal control system fails to recognize them and react appropriately. Likewise, unrecognized and/or improperly managed changes in the operation of existing controls — such as new people, processes, and technology — could render the internal control system ineffective.
35. In order to consider the effect of change on internal control systems, organizations should begin the monitoring process in a given risk area with a supported baseline of known effective control. With the baseline as a starting point, organizations can design ongoing monitoring and separate evaluations to identify and address changes as they occur. This concept is outlined below and illustrated in Figure 6.

1. **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. An established baseline understanding of internal control effectiveness provides an appropriate starting point for more-effective and more-efficient monitoring. Figure 6 shows the control baseline as the starting point and a new control baseline established over time through monitoring.

2. **Change Identification** — Internal controls change from their baseline for one of two reasons: (1) The operation of the existing controls change, or (2) the underlying processes or risks change due to internal or external factors that lead to a necessary modification in the design of internal controls. In either case, these changes, if not properly managed, are the catalyst for internal control failures.

   The risk assessment component\(^\text{14}\) 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,\(^\text{15}\) 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 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 below).

---

\(^{14}\) 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.”

\(^{15}\) See Ongoing Monitoring and Separate Evaluations on page 38 for further discussion.
3. **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.

4. **Control Revalidation** — When ongoing monitoring procedures use highly persuasive information, 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.

36. All four components of this structure contribute to the effectiveness of an organization’s monitoring program. The second and third components (change identification and change management) warrant further discussion as they contribute to the efficiency of monitoring and, thus, to the efficiency of internal control. Effective change-identification and change-management processes provide important information to evaluators that influences their assessment of the risk that controls will fail to manage or mitigate risk — information about changes that should be made in controls because the underlying processes or risks change, and information about changes in controls that have already taken place, such as changes in personnel performing controls. As a result, change-identification and change-management processes can influence the scope of other monitoring procedures that may be more costly.

---

16 See the discussion of persuasive information beginning on page 27.
17 See the Ongoing Monitoring and Separate Evaluations section beginning on page 38
Applying the Concepts

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 would begin 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 normal business practice of being aware of the implications of new sales channels or of changes in the order-entry system programming.

Monitoring for changes in the operation of controls 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 routinely, with little change, as a normal part of business operations. If the supervisor identifies a change, he or she could 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 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 important order-entry controls are operating correctly. Such revalidation would occur periodically, commensurate with the level of risk.
III. Designing and Executing Monitoring Procedures

37. The core of effective and efficient monitoring lies in designing and executing monitoring procedures that evaluate important controls over meaningful risks to the organization’s objectives.

38. An organization will face many risks that threaten the achievement of its objectives, but risk levels and potential consequences vary. The likelihood of occurrence for one risk may be remote. The impact of another risk may be inconsequential to the objective even if the likelihood of the occurrence is high. Therefore, meaningful risks are those that might reasonably have a consequential effect on an organizational objective.

39. Just as risks vary in their ability to affect an organization’s objectives, the controls that manage or mitigate those risks vary in their importance. In one sense, every implemented control is important — organizations generally do not implement controls they do not need. However, in the context of monitoring the effectiveness of an internal control system, evaluators typically focus their efforts on those controls that, when monitored, provide the level of support needed to conclude that the internal control system is effective in addressing the identified meaningful risk(s).

40. In order to implement monitoring that provides the necessary level of support, organizations must determine three things:

- What controls to monitor,
- What monitoring procedures to employ, and
- How often to employ them.
41. A practical way to view this decision process is to follow its logical progression, demonstrated in Figure 7.

42. The components in this illustration are discussed in detail in later sections, but summarizing them here may be helpful.

43. Designing monitoring begins with understanding and prioritizing the risks to achieving important organizational objectives. Prioritizing risks helps identify which risks are meaningful enough to subject to control monitoring. Depending on the purpose of the monitoring, this process might identify different risks at different organizational levels. For example, monitoring of controls that prevent theft of supplies might be meaningful to a store manager, but might not warrant the individual attention of the Chief Executive Officer (CEO).

44. Risk prioritization is a natural part of the risk assessment component of internal control. Its inclusion here is not meant to imply the necessity of a separate risk assessment function dedicated solely to support the monitoring function. In a properly operating internal control system, the risk assessment component will routinely identify and prioritize risks to the organization’s objectives. This information will then influence decisions regarding the type, timing, and extent of monitoring.
45. The next step is to determine the controls that are important in managing or mitigating the identified meaningful risks.

46. Important controls — often referred to as key controls — are those that are most important to monitor in order to support a conclusion about the internal control system’s ability to operate effectively. They often have one or both of the following characteristics:

- Their failure might materially affect the organization’s objectives, yet not reasonably be detected in a timely manner by other controls, and/or
- Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization’s objectives.

47. Identifying key controls helps ensure that the organization devotes monitoring resources where they can provide the most value.

48. Once key controls are noted, 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 working properly.

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

### Understand and Prioritize Risks

50. As part of the risk assessment component of internal control, 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.

51. 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. The process begins at the entity level and drives down to an appropriate level of detail within the organization. Once completed, the effort to maintain this risk assessment might involve scanning the environment routinely for changes and only periodically conducting a full risk assessment update.

52. The assessment of risk importance might be based on a significance-and-likelihood analysis or a less formal prioritization process. 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\(^{19}\) risk as “low” — based on the expectation that the internal control system will prevent or detect such activity — would be inappropriate. Considering risk importance apart from expected control effectiveness helps ensure that the organization monitors controls it relies on most to address meaningful risks.

53. For each important objective and risk, the organization might identify locations, operations or processes where risks could manifest in a material way.

54. 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, and information system complexity.

- **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** — The presence of valuable assets (e.g., cash, trade secrets, fungible goods, etc.) and the possibility for fraudulent activity (e.g., through access to systems, execution of unauthorized transactions, or management override of controls) are risk factors that increase the need for strong internal controls and related monitoring.

\(^{19}\) 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

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. Understand and Prioritize Risk

<table>
<thead>
<tr>
<th>Area</th>
<th>Objective</th>
<th>Risk</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>1. Recognize in the proper period</td>
<td>Overstatement – recording revenue before delivery or title transfer</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

**Rationale:**
- 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 recognition before a shipment leaves the warehouse

Conversely, 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.)

<table>
<thead>
<tr>
<th>Area</th>
<th>Objective</th>
<th>Risk</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>2. Recognize revenue in proper amounts</td>
<td>Overstatement – sales agents grant future credits for unsold goods (i.e., “channel stuffing”)</td>
<td>High</td>
</tr>
</tbody>
</table>

**Rationale:**
In this example, 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.

Note that the personnel responsible for this risk assessment process first identified the important objectives and the risks to achieving those objectives. Then they thought rationally through the risk, considering factors that might increase or decrease the likelihood and/or significance of the risk.

**Understand the Internal Control System and Identify Key Controls**

55. In order to identify the important or 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. As noted earlier, every control may be important to the internal control system, but some are more important to monitor than others in order to support a conclusion that the internal control system is effective.

56. 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 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 three related processes.
57. The discussion of key controls in this guidance is not intended to establish different classes of internal control. Rather, it is to help organizations understand how they might reasonably conclude that the internal control system is effective in addressing a given risk by focusing monitoring efforts on a subset of controls. This concept can operate at varying levels within an organization. Thus, a control that is “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. The goal is to identify those controls that, when monitored, will provide the necessary level of support regarding the effectiveness of the internal control system.

58. 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 and, therefore, need to be subjected to an appropriate level of monitoring when they are important to addressing meaningful risks. The table on page 33 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 evidence demonstrates that corrective actions have effectively addressed the cause of the control failure.
Applying the Concepts

Continuing the revenue recognition example from page 21, 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 the monitoring first understand how the internal control system addresses the risk. They can then identify the controls that (when monitored) 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 ability to address 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 below 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. Understand the Internal Control System and Identify Key Controls

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

#### June 2008

<table>
<thead>
<tr>
<th>Key</th>
<th>Control</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Approval of sales above a certain limit</td>
<td>Control Activity</td>
</tr>
</tbody>
</table>

**Rationale:**

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.

| 8. | Exception reports generated and reviewed for any transactions exceeding authorized limits | Control Activity & 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 |

**Rationale:**

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.

| 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 |

**Rationale:**

This is a dual-purpose control (i.e., a control activity identifying possible revenue recognition errors and a monitoring activity using indirect information) that might 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.
Identify Persuasive Information

59. The **persuasiveness of information** refers to the degree to which the monitoring 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, determining the necessary level of persuasiveness requires those responsible for monitoring to exercise judgment.

60. 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*

61. 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.

62. 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.
63. 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).

64. **Relevance of information** — Information is relevant when it tells the evaluator something meaningful about the operation of the underlying controls or control component. For example, reviewing résumés and training records can tell an evaluator something about whether an accountant has the 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.

65. Information that directly confirms the operation of controls is more relevant than information that merely allows the evaluator to infer whether the controls are working. 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).

66. **Direct information** substantiates the operation of controls. It is obtained by observing controls in operation, reperforming them, or otherwise directly testing their operation, and can be useful in both ongoing monitoring and separate evaluations. Generally, direct information is highly relevant because it provides an unobstructed view of control operation.

---

20 Observing controls in operation is an important monitoring tool when applied properly. In fact, observation may be the only available method of evaluation in situations where a control does not result in some form of documentation that can be evaluated after the fact. For example, a weekly management meeting where past-due receivables are discussed may be an important control in forming proper judgments about receivable collectibility and necessary reserve amounts. 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.
67. **Indirect information** is all other information used to infer whether controls or control components continue to operate effectively. It either relates to, or is produced by, the process in which the controls reside. Indirect information might include, but is not limited to, (1) operating statistics, (2) key risk indicators, (3) key performance indicators, and (4) comparative industry metrics.

68. Indirect information is used to identify anomalies that indicate that a control, or set of controls, may have failed to operate properly. The absence of such anomalies, however, does not demonstrate explicitly to evaluators that underlying controls are effective. As a result, there is a limit to the level of support (i.e., persuasiveness) that indirect information can provide on its own, especially over a long period of time.

69. In an internal control system where the evaluator begins with a baseline of direct information establishing that the controls in question are effective, 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.

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

71. 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 infer that the risk of control failure in the billing area is reduced to an acceptable level, at least for some period of time.
conclusion might then influence the type, timing, and extent of other monitoring procedures over controls in the billing area.

72. 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.

<table>
<thead>
<tr>
<th>Factor to Consider</th>
<th>Possible Impact on the Use of Direct vs. Indirect Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential impact of a control's failure</td>
<td>As the potential impact of a control failure increases, the need to monitor using direct information increases.</td>
</tr>
<tr>
<td>Length of time since control was last evaluated through direct information</td>
<td>Over time, indirect information can lose 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. In addition, indirect information can be obscured by normal changes and operating factors. Thus, monitoring using indirect information should be reconfirmed periodically through monitoring of direct information.</td>
</tr>
<tr>
<td>Controls that operate in areas with a high degree of change in people, processes, or technology versus controls operating in stable areas</td>
<td>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.</td>
</tr>
<tr>
<td>The relative persuasiveness of the indirect information</td>
<td>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 by salesperson, by customer provides more-persuasive information about the related controls than does a review of sales trends solely at the consolidated company level.</td>
</tr>
<tr>
<td>The effectiveness of the follow-up process</td>
<td>Indirect information is useful in monitoring only if the organization actually examines identified anomalies and considers the control implications if problems are noted.</td>
</tr>
</tbody>
</table>

73. **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.

74. Although accuracy and verifiability are commonly understood, objectivity of information sources warrants further discussion.
75. The “Characteristics of Evaluators” section discussed the objectivity of the evaluator. This section discusses objectivity in relation to the evaluator’s 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.

76. 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).

77. 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 currently 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

78. 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:

<table>
<thead>
<tr>
<th>Factor to Consider</th>
<th>Possible Impact on the Amount of Information Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential impact of a control's failure</td>
<td>As with decisions regarding the use of direct vs. indirect information discussed on page 30, the potential impact of a control's failure may also 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 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.</td>
</tr>
<tr>
<td>Controls that operate in areas with a high degree of change in people, processes, or technology versus controls operating in stable areas</td>
<td>Also consistent with decisions regarding the use of direct vs. indirect information, 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.</td>
</tr>
<tr>
<td>Control frequency</td>
<td>Controls that occur infrequently are often subjected to judgmental selection methods, while those that occur frequently lend themselves to possible statistical sampling methods. In judgmental methods, organizations determine the amount of information to evaluate after considering the level of risk and the importance of the identified control.</td>
</tr>
<tr>
<td>Who is conducting the monitoring</td>
<td>If evaluators are routinely involved in or witness the execution 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 — and thus more objective — they typically need to obtain more information regarding the controls’ operation.</td>
</tr>
</tbody>
</table>
### 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 to gather and evaluate regarding Control B. For example, effectively monitoring a three-way-match control between purchase orders, receiving documents, and invoices may help support a conclusion that data-entry controls over invoices are effective, which may influence the scope of monitoring over 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 (versus unintentional failure) 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.

---

79. 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

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 allow us to infer that it may be operating properly 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 we last obtained information that directly supported our control conclusions, and
  - Effectiveness of other controls that might address the same risk(s)?
- Do we have a reasonable basis for concluding that the information we are using 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 evaluation of the information taking place in a time frame that will allow us to take corrective action before a control breakdown has a reasonable opportunity to materially impact the organization’s related objectives?
- Does the information relate to the period under consideration? (For example, information may be too old to tell us anything about the current operation of controls, or it might come from a period following the desired control evaluation date.)
• Do we gather and evaluate enough information to support our control conclusions? (Note: the answer might be influenced by some of the factors listed in the table on page 32.)

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.
<table>
<thead>
<tr>
<th>Key Control</th>
<th>Available Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control #1 – Tone from the top</td>
<td>- Management participation and periodic communications in sales meetings, including setting expectations that specifically address this risk and others</td>
</tr>
<tr>
<td></td>
<td>- Evidence of corrective actions, if necessary</td>
</tr>
</tbody>
</table>

Rationale:
Relevant – This information is obtained from witnessing or delivering the communications, so it is relevant.
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.
Timely – The observations happen in real time and would be timely.
Sufficient – Witnessing these communications and actions would adequately demonstrate the existence of a proper tone from the top.

| Control #6 – Approval for contract modifications | - Signed approval noted on modified contract                                           |
|                                                | - Participation by the CFO in sales meetings where modifications are discussed        |

Rationale:
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 information if such modifications are a standard discussion topic.
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 all 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.
Note that objectivity could be a factor to consider here. If the sales manager was the person signing approvals and participating in the sales meetings, then the CFO may want a more objective, periodic evaluation.
Timely – The timeliness of any approval review process will be dependent on the evaluator’s selecting 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.
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 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).
### Key Control

<table>
<thead>
<tr>
<th>Control #10 – Sales personnel compensation review &amp; adjustment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation by the CFO in the review/adjustment process</td>
</tr>
<tr>
<td>Completed and documented reviews/adjustments</td>
</tr>
</tbody>
</table>

**Rationale:**
- 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.
- Reliable – Both forms of information above would reliably tell the evaluator whether this control was working. Again, objectivity could be a factor to consider.
- Timely – Similar to Control #6, timeliness depends on the evaluator’s selecting the right instances of the control to evaluate. Participation in the process is real-time and, thus, is timely.
- Sufficient – Deciding how much of this information to gather will follow a similar thought process as Control #6.

<table>
<thead>
<tr>
<th>Control #11 – Sales and return trend review on a by-salesperson, by-customer basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation by the CFO in the review process</td>
</tr>
<tr>
<td>Completed and documented sales and return trend review</td>
</tr>
</tbody>
</table>

**Rationale:**
The rationale for concluding on the persuasiveness of this information will be similar to the rationale for concluding on the information in Control #10.

### Other Possibly Persuasive Information

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue would increase, coupled with declining margins over time</td>
</tr>
<tr>
<td>Increase in accounts receivable aging on a per-salesperson basis</td>
</tr>
<tr>
<td>Increase in sales returns after quarter-end</td>
</tr>
</tbody>
</table>

**Rationale:**
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.
Implement Monitoring Procedures

80. With the risks prioritized, key controls selected, and the available persuasive information identified, the organization implements monitoring procedures that evaluate the effectiveness of the internal control system’s ability to manage or mitigate the identified risks. 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

81. Ongoing monitoring procedures using both direct and indirect information are built into the normal, 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 monitor 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.  

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

---

21 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."
83. Separate evaluations are often performed by people who are not directly responsible for the operation of the controls being monitored. As such, they may provide a more objective analysis of control effectiveness than ongoing monitoring procedures that are often performed by less objective personnel.

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

85. Principle 19 of COSO’s 2006 Guidance, 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 normal operating activities and automated monitoring routines.

- Provides objective assessments — Ongoing monitoring and/or separate evaluations provide an objective consideration of internal control effectiveness.

- Uses knowledgeable personnel — Evaluators understand the components being evaluated and how those components relate to the organization’s objectives.

- Considers feedback — Management and the board receive feedback on the effectiveness of internal control.

---

**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.”

---

22 See Appendix A.

23 COSO’s 2006 Guidance refers specifically to internal control over financial reporting, but these attributes are applicable to monitoring all COSO objectives.

24 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.
• Adjusts scope and frequency—Management varies the scope and frequency of separate evaluations, depending on the significance of risks being controlled, the importance of the controls in mitigating those risks, and the effectiveness of ongoing monitoring.

86. 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).

87. To determine how often separate evaluations will be performed, organizations consider the likelihood and significance of the risk’s occurrence between evaluations, including consideration of the support provided by ongoing monitoring. As the level of risk increases/decreases, the interval between separate evaluations decreases/increases.

88. 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\(^{25}\)) and primarily for independent confirmation that the ongoing monitoring procedures are working.

89. 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.

**Monitoring Controls Outsourced to Others**

90. When organizations use external parties to perform certain functions, such as a bank outsourcing loan servicing or a corporation outsourcing its benefit plan administration, the associated risks 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 those risks that are meaningful, and obtain at least periodic confirmation

\(^{25}\) See the 1992 COSO Framework, page 70.
that those controls are operating effectively. In some cases, the service provider may have an independent audit performed of the controls that are relevant to the user organization. Such an audit can serve as an effective periodic separate evaluation of identified key controls in place at the service provider. Where such an audit is not available and where the level of risk warrants, user organizations may determine to conduct their own periodic separate evaluations of key controls. In fact, a “right to audit” clause is often included in contracts between user and service organizations.

**Using Technology for Monitoring**

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

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

- **Transaction data** — Comparing processed transaction (or masterfile) data against a set of control rules 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 possible the verification that changes are appropriate and authorized.

- **Processing integrity** — Verifying and monitoring the completeness and accuracy of data as it progresses through various IT processes and systems.

- **Error management** — Monitoring the volume and resolution of activity in suspense areas, error logs, or exception reports, typically as part of an application system.
93. **Process management tools** — Process management tools are designed to make monitoring more efficient and sustainable by automating some monitoring activities, including assessing risks, defining and evaluating controls, and communicating results. These tools are most often used in situations in which responsibilities for controls are distributed throughout multiple or geographically dispersed business units, but they can also be of value to any organization—including smaller ones. Most of these tools use workflow techniques to provide structure and consistency to the performance of monitoring procedures. Some features that make these tools useful include their ability to:

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

94. Some control monitoring tools 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, electronically identifying segregation of duties issues, etc.). 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.

### Applying the Concepts

The “Understand and 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 show how those control-importance determinations might also affect the monitoring procedures employed and the information used in monitoring.
### Control Importance | Determining Factors | Possible Monitoring Approach
--- | --- | ---
**Highest**<br>Controls that:<br>– are susceptible to a high risk of failure, and<br>– address risks deemed to be high-priority | Ongoing monitoring using direct and indirect information, with periodic separate evaluations of direct information

**Moderate in short term**<br>Controls that:<br>– are less susceptible to failure, and<br>– address risks deemed to be high-priority | Ongoing monitoring using indirect information, with periodic separate evaluations of direct information

**Moderate in long term**<br>Controls that:<br>– are susceptible to a high risk of failure, and<br>– address risks deemed to be lower-priority | Ongoing monitoring using indirect information, with less-frequent separate evaluations of direct information

**Lowest**<br>Controls that:<br>– are less susceptible to failure, and<br>– address risks deemed to be lower-priority | 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

<table>
<thead>
<tr>
<th>Key Control</th>
<th>Monitoring Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control #1 – Tone from the top</strong></td>
<td>&lt;ul&gt;– The CFO participates in the monthly sales meeting, both establishing and verifying the proper tone from the top.&lt;br&gt;– Internal audit also observes these meetings periodically.&lt;/ul&gt;</td>
</tr>
</tbody>
</table>

**Rationale:**<br>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.
<table>
<thead>
<tr>
<th>Key Control</th>
<th>Monitoring Procedure</th>
</tr>
</thead>
</table>
| Control #6 – Approval for contract modifications | - Participation by CFO in monthly sales meetings.  
- Controller (or internal audit) to select X contracts every quarter, noting any unapproved modifications. |
| Rationale:                                      | 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. |
| Control #10 – Sales personnel compensation review & adjustment | - CFO participation in this control is sufficient.  
- Audit committee to direct annual testing by internal audit. |
| Rationale:                                      | 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. |
| 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. |
| Rationale:                                      | 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. |

**Other Considerations**

<table>
<thead>
<tr>
<th>Monitoring Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional periodic test</td>
</tr>
<tr>
<td>Rationale:</td>
</tr>
</tbody>
</table>
IV. Assessing and Reporting Results

95. The monitoring process is complete when the results are compiled and reported to the 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:\(^{26}\)

- 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.\(^{27}\)

96. 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.

Prioritizing and Communicating Results

97. Consistent with Principle 20 of COSO’s 2006 Guidance, monitoring includes identifying 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 regarding 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 result in an error — The fact that a deficiency has been identified means that there is at least some likelihood that an error could occur. The greater that likelihood, the greater the severity of the control deficiency.

\(^{26}\) See COSO’s 2006 Guidance, page 94.
\(^{27}\) See footnote 6 on page 3.
• The effectiveness of other, **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 potential effect of an identified deficiency on organizational objectives — As an identified deficiency’s potential effect increases, its severity increases.

• The potential effect of the deficiency on other objectives — Beyond consideration of the above factors, organizations may consider the effect of a deficiency on their overall operating effectiveness or efficiency. For example, an identified deficiency may prove to be immaterial in relation to the financial reporting objective, but it may cause inefficiencies that warrant correction in relation to operational objectives.

• 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.

98. 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 objective personnel.

**Applying the Concepts**

The following table describes how organizations might consider the likelihood and significance variables as they prioritize identified control deficiencies. Smaller, less complex organizations might perform this ranking process 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.

It should be noted that 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.
Reporting Internally

99. 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 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 profitability.

100. Some monitoring, however, is conducted for purposes that might be material only to a small part of an organization, e.g., a small subsidiary’s operational monitoring to meet local goals that are not material to the consolidated company. Identified deficiencies in this case might have “higher likelihood” and “higher significance” relative to the subsidiary’s objectives, but not to the overall organization’s. In such situations, reporting might be limited to local management personnel for whom the local goals are important.

101. 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.

102. 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 where appropriate.

**Applying the Concepts**

The risk assessment process described in the “Understand and 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.

**Reporting Externally**

103. A properly designed and executed monitoring program helps support external assertions because it provides persuasive information that internal control operated effectively at a point in time or during a particular period.

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

A properly designed and executed monitoring program helps support external assertions.

105. 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 find it helpful to compare the scope of its monitoring program with the needs of external parties, such as auditors and regulators, to ensure that all parties understand and agree on the general
requirements. 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.

**Potential Modifications to Monitoring**

106. 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.

107. 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 evidence. The most cost-effective option may be implementing a more objective monitoring process, thereby making the external party’s work more efficient.

108. 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. For example, an organization’s external auditors may determine, based on their audit plan, to test 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 of 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 the independent audit.
V. Scalability of Monitoring

109. 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

110. 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), all of which “roll up” to a home office or headquarters, and are typically 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.

---

28 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 not meant to imply that the CFO is at the head of every monitoring program.
111. 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 implicit knowledge of the operation of controls. Monitoring in the smaller organization (Figure 10) can look much like monitoring at lower levels 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, whereas the lead evaluator in the smaller organization performs more monitoring of actual internal controls. This increase in implicit knowledge about the operation of internal control may allow the evaluator in a smaller organization to support his or her control conclusions through less-intense monitoring than would be necessary in a larger organization where the evaluator is further removed from the operation of controls.

112. Large companies 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, a company 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 critical internal controls. In addition, management’s objectivity in a smaller organization may be impaired by the fact that it performs some of the control activities that are subject to monitoring, thereby increasing the importance of monitoring performed by the board or audit committee.

**Scalability Based on Complexity**

113. 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).

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

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

**Formality of Monitoring and Level of Documentation**

116. 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.

117. When external reporting requirements exist, however, organizations of all sizes, especially smaller ones, may find that more-formal documentation is a cost-effective way to improve the efficiency of meeting those requirements. For example, an external auditor may be able to conduct a more efficient audit if he or she has access to documentation that demonstrates the results of management’s monitoring.

118. 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.

**Applying the Concepts**

When external reporting requirements exist, management may design ongoing monitoring such that it provides the majority of evidence management needs to support its assertions, possibly reducing the extent of year-end, separate evaluations whose sole purpose is to support the external assertions.
In considering the impact of external assertion requirements on monitoring, management and the board — possibly through discussion with their auditor or regulator — might consider the following:

- Are there any elements of the assertion requirement that might cause us to perform more-extensive monitoring in a particular area than we feel is necessary given our assessment of risk and control importance analysis? If so, a review of the regulatory requirement (to make sure it does, in fact, require such an evaluation) and the risk assessment process (to make sure the organization did not omit an important risk and related control from normal monitoring consideration) may be in order. (Note that, while such conflicts should be rare, they may occur in some regulated environments.)

- Does the documentation adequately support the assertions?

- 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?

- 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 testing so that the third party can use the results to support its conclusions)?

VI. Assessing the Effectiveness and Efficiency of Monitoring

119. 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.

120. As the COSO Framework indicates, the monitoring component of internal control “ensures that internal control continues to operate effectively.” 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.

---

29 COSO Framework, p. 69.
<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the organization appropriately considered all of the risks that could materially affect its objectives? 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?</td>
<td>Is the organization monitoring controls at a cost, effort, or organizational level that is inconsistent with the amount of risk the controls mitigate?</td>
</tr>
<tr>
<td>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?</td>
<td>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.)</td>
</tr>
<tr>
<td>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?</td>
<td>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 intensity over time (e.g., using indirect information over longer periods of time between control baselines established using direct information)?</td>
</tr>
<tr>
<td>What do the results of internal audits, external audits, or regulatory exams tell the organization about the effectiveness of monitoring? Have they uncovered control deficiencies not identified by monitoring?</td>
<td>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?</td>
</tr>
</tbody>
</table>
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 companies 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.
Glossary

Accuracy  The degree to which information can reasonably be expected to be free from error and/or to communicate results that reflect reality.

Board monitoring  Board monitoring is the execution of monitoring procedures by the board, its committees, or others charged with overseeing management conduct. It involves the oversight of management’s performance in relation to all of the COSO components, including evaluating management’s own monitoring process. It also includes procedures to evaluate the effective operation of those controls that senior management cannot monitor objectively, such as controls performed directly by senior management and controls that are at risk of management override.

Compensating controls  Controls that accomplish the same objective as another control and that can be expected to “compensate” for deficiencies in that control.

Competence  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. They help ensure that necessary actions are taken to address risks to achieving objectives. Control activities occur throughout the organization, at all levels, and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
Control baseline  
A control baseline is a point in time at which an organization has persuasive information supporting a reasonable conclusion that controls across the entire organization or in a given area are 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  
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:

- The integrity, ethical values, and competence of the entity’s people;
- Management’s philosophy and operating style;
- The way in which management assigns authority and responsibility, and in which it organizes and develops its people; and
- The attention and direction provided by the board of directors.

Control objectives  
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.

Deficiency or internal control deficiency  
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.
Direct information

Direct information is information that directly substantiates the operation of controls and is obtained by observing them in operation, reperforming them, or otherwise directly evaluating their operation. Direct information is generally highly persuasive because it provides an unobstructed view of control operation. It can be obtained from either ongoing or separate evaluations, but it must link directly to a judgment regarding the effective operation of controls.

Evaluator

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 skills, knowledge, and authority 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.

Indirect information

Indirect information is information (other than direct information) that is relevant to assessing whether an underlying risk is mitigated and controls are operating. Indirect information does not tell the evaluator explicitly that underlying controls are operating effectively, but in the presence of an effective monitoring structure (including a baseline understanding of internal control effectiveness, change-identification/management procedures, and periodic control reconfirmation), persuasive indirect information can influence the type, timing and extent of monitoring procedures using direct information.
Information and communication refer to the nerve-center function of an internal control system. Pertinent information — internal and external — must be identified, captured, and communicated in a form and time frame that enable personnel to carry out their responsibilities. Information systems use or produce reports containing operational, financial, and compliance-related information, all of which make it possible to operate and control the business. Effective communication must also occur in a broader sense, flowing down, across, and up the organization’s structure. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal control is a process effected by an entity’s board of directors, management, and other personnel, and it is designed to provide reasonable assurance that organizational objectives can be met.

Key controls are those that are most important to monitor in order to support a conclusion about the internal control system’s ability to manage or mitigate meaningful risks. They often have one or both of the following characteristics:

- Their failure might materially affect the organization’s objectives, yet not reasonably be detected in a timely manner by other controls, or
- Their effective operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization’s objectives.

Identifying key controls helps ensure that the organization devotes monitoring resources where they can provide the most value.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key performance indicators</td>
<td>Key performance indicators are metrics that reflect critical success factors. They help organizations measure progress towards goals and objectives.</td>
</tr>
<tr>
<td>Key risk indicators</td>
<td>Key risk indicators are forward-looking metrics that seek to identify potential problems, thus enabling an organization to take timely action, if necessary.</td>
</tr>
<tr>
<td>Material or materiality</td>
<td>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, <em>Journal of Accounting Research</em>). In a financial reporting context, an error is material if it would be reasonable to conclude that a user of financial statements would alter his or her decisions as a result of the identified intentional or unintentional error.</td>
</tr>
<tr>
<td>Objective or objectivity</td>
<td>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.</td>
</tr>
<tr>
<td>Ongoing monitoring</td>
<td>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.</td>
</tr>
<tr>
<td>Persuasiveness of information or persuasive information</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 that are linked at different levels and internally consistent. Risk assessment is the identification and analysis of risks relevant to realizing objectives, and it serves as a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, flexible mechanisms are needed to identify and address the special risks associated with change.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-assessment</td>
<td>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.</td>
</tr>
<tr>
<td>Self-review</td>
<td>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.</td>
</tr>
<tr>
<td>Separate evaluations</td>
<td>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.</td>
</tr>
<tr>
<td>Sufficient information</td>
<td>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.</td>
</tr>
<tr>
<td>Suitable information</td>
<td>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).</td>
</tr>
<tr>
<td>Timely information</td>
<td>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.</td>
</tr>
<tr>
<td>Verifiable or verifiability</td>
<td>Verifiable information is information that can be established, confirmed or substantiated as true or accurate.</td>
</tr>
</tbody>
</table>