2009

COSO Internal control - integrated framework: Guidance on monitoring internal control systems, Volume 1: Guidance

Committee of Sponsoring Organizations of the Treadway Commission

Committee of Sponsoring Organizations of the Treadway Commission

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

www.coso.org

COSO

COMMITTEE OF SPONSORING
ORGANIZATIONS OF THE TREADWAY COMMISSION

Internal Control — Integrated Framework

Guidance on Monitoring Internal Control Systems

Volume I : Guidance

990021

monitoring

Guidance on Monitoring Internal Control Systems

Volume I: Guidance

January 2009

2 3 4 5 6 7 8 9 0 PIP 1 9 8 7 6 5 4 3 2 1 0

Additional copies of this work may be obtained by visiting www.cpa2biz.com.

ISBN 0-87051-795-3

From the Chairman …

The COSO Board is pleased to issue its *Guidance on Monitoring Internal Control Systems* (the Monitoring Guidance) — a demonstration of COSO's commitment to assisting organizations in implementing effective internal control and monitoring its continued effectiveness. The Board believes that organizations can achieve greater efficiency and effectiveness through a better understanding and more efficient utilization of the monitoring component of the COSO *Internal Control — Integrated Framework* (the COSO Framework). The purpose of the guidance is to assist organizations in monitoring the effectiveness of their internal control systems and taking timely corrective actions as needed.

The COSO Framework contemplates that monitoring is implemented as an active part of an organization's internal control system. Thus, an organization should consider whether monitoring of internal control should be performed annually — as often occurs in firms that report publicly on the quality of their internal control — or whether monitoring can be "built into" the organization's everyday activities. The COSO Board believes that many organizations can achieve greater efficiencies by building monitoring into their ongoing internal control processes. The guidance seeks to equip organizations to attain that goal.

The Grant Thornton project team, accompanied by a large, diverse task force, grappled with a number of conceptual and practical issues in developing the Monitoring Guidance. The team addressed basic issues such as, "How can an organization know that its monitoring activities are effective?" and more-complex issues such as, "To what extent can an organization utilize 'indirect information' (e.g., comparisons with expectations) as part of an effective monitoring program?" Readers of the guidance will find that effective monitoring is both risk based and principles based and that the guidance is presented in a way that encourages adaptation to individual organizational circumstances.

I want to thank the entire Grant Thornton team and the task force for their contributions in developing the Monitoring Guidance. In particular, I want to recognize Trent Gazzaway, Grant Thornton's Managing Partner of Corporate Governance, for leading this project and for his intellectual contributions and perseverance. His attention to detail was instrumental in ensuring consistency with the COSO *Internal Control — Integrated Framework,* as well as with the COSO 2006 guidance for smaller public companies.

We hope you will find the Monitoring Guidance useful. We always welcome your feedback, including examples of areas in which you have successfully implemented monitoring.

Sincerely,

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

I. Purpose of the Guidance

1. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) introduced the *Internal Control — Integrated Framework* (the COSO Framework) in 1992. Much has happened since the initial release. Most notably, some countries have implemented regulations requiring certain companies to publicly report on the effectiveness of internal control.

COSO's Guidance on Monitoring Internal Control Systems (COSO's Monitoring Guidance) elaborates on the monitoring component of internal control discussed in the 1992 COSO Framework and in the subsequent *Internal Control over Financial Reporting — Guidance for Smaller Public Companies* issued in 2006 (COSO's 2006 Guidance).

2. COSO initiated this project based on observations that many organizations were not fully utilizing the monitoring component of internal control. This fact became most clear as COSO witnessed the efforts of many companies to meet internal control certification and assertion requirements around the world.

3. COSO observed that some organizations had effective monitoring in certain areas, but were underutilizing the results of that monitoring to support their conclusions about the effectiveness of internal control, especially conclusions related to the effectiveness of internal control over financial reporting. Instead, they were adding redundant, often unnecessary procedures designed to evaluate controls for which management — through its existing monitoring efforts — already had sufficient support. Other organizations were not making the best use of **ongoing monitoring**[1] procedures or lacked necessary monitoring procedures altogether, which may have caused them to implement inefficient year-end evaluations to support their conclusions about the effectiveness of internal control.

4. The objectives of COSO's Monitoring Guidance are twofold:

- *To help organizations improve the effectiveness and efficiency of their internal control*[2] *systems*. The COSO Framework emphasizes that organizations with effective internal control systems monitor the effectiveness of those systems over time[3] — just as a manufacturing organization monitors the continued effectiveness and efficiency of its manufacturing procedures. This guidance is designed to help organizations

---

1 See the Glossary in Volume II for definitions of terms set in boldface.

2 Throughout this document, we use the terms "controls" and "internal controls" to refer to all of the components of the internal control framework, i.e., the term is used to reference more than just the control activities component.

3 COSO Framework, p. 69.

recognize and maximize the use of monitoring when it is effective and enhance monitoring in areas where improvement may be warranted.

- *To provide practical guidance that illustrates how monitoring can be incorporated into an organization's internal control processes.* The "Applying the Concepts" sections in Volume II of the guidance provide easy reference points — demonstrating how organizations might apply the general concepts of monitoring. Volume III goes further by providing a variety of monitoring examples from organizations interviewed during the project.

5. This guidance does not:

- Change the COSO Framework or COSO's 2006 Guidance,
- Dictate risks or controls that organizations must consider,
- Mandate the exact monitoring procedures that organizations must follow,
- Increase the monitoring effort for organizations in areas where monitoring is already effective, or
- Mandate a certain level or formality of monitoring documentation, including the use of certain terms.[4]

6. This guidance should help management, board members, internal and external auditors, regulators, and others recognize effective monitoring where it exists and take into account its results with respect to their duties. In areas where monitoring is ineffective, this guidance should help organizations identify and correct weaknesses and move toward achieving effectiveness in monitoring. In so doing, organizations can improve their internal control system's ability to provide reasonable assurance about the achievement of organizational objectives. Effective monitoring may also result in organizational improvements by (1) minimizing internal control failures and their errors/defects that require correction, and (2) improving the quality and reliability of information used for decision making.

7. 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 its initial application may be related to evaluating internal control over financial reporting (ICFR), most of the examples concentrate on the financial reporting objective.

---

[4] This guidance uses terms such as "meaningful risk," "persuasive information," "key controls," and "direct and indirect information." These terms, and others, are defined in this guidance and the Glossary at the end of Volume II. Their use is intended to make the guidance understandable to a broad audience. It is not intended to force changes in the terminology organizations use when discussing or documenting monitoring.

8. The Monitoring Guidance comprises three volumes. Volume I, the Guidance volume, is designed to demonstrate succinctly the core concepts embodied in COSO's monitoring component. Volume II, the Application volume, is integral to Volume I and contains a more detailed description of the principles contained in Volume I. The Application volume should be read by those responsible for implementing the guidance and by those who are interested in gaining a greater understanding of the related concepts. Volume III, the Examples volume, contains examples from organizations whose monitoring efforts are consistent with the Monitoring Guidance.

II. Nature and Purpose of Monitoring

9. The COSO Framework states that "monitoring ensures that internal control continues to operate effectively."[5] COSO's 2006 Guidance enhances the understanding of monitoring by articulating the following two related principles:

See Vol. II, ¶¶ 1–2.

- Ongoing and/or **separate evaluations** enable management to determine whether the other components of internal control[6] continue to function over time.
- 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.

10. COSO's Monitoring Guidance builds on those two fundamental principles.

11. The COSO Framework recognizes that risks change over time and that management needs to "determine whether the internal control system continues to be *relevant* and able to *address new risks.*"[7] Thus, monitoring should evaluate (1) whether management reconsiders the design of controls when risks change, and (2) whether controls that have been designed to reduce risks to an acceptable level continue to operate effectively. Accordingly, this guidance continues to emphasize COSO's belief that monitoring should be based on an analysis of risks to organizational objectives and an understanding of how controls may or may not manage or mitigate those risks.

See Vol. II, ¶¶ 38–41.

---

[5] COSO Framework, p. 69.

[6] COSO's 2006 Guidance refers specifically to internal control over financial reporting, but the concepts can be applied to any internal control objective.

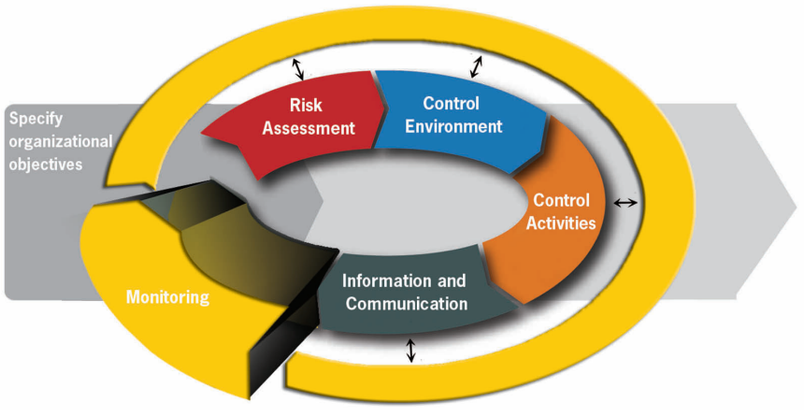
[7] COSO Framework, p. 69, emphasis added.

12. An overview of the framework and how its components work together is shown in Figure 1, which is an enhancement of the process approach to internal control developed in COSO's 2006 Guidance. The enhancements include the explicit recognition that monitoring relates to all three internal control objectives and not just to the financial reporting objective.

See Vol. II, ¶¶ 11–19.

13. This graphic also demonstrates that monitoring evaluates the internal control system's ability, in its entirety, to manage or mitigate **meaningful risks** to organizational objectives.

14. Each of the five components of internal control set forth in the COSO Framework is important to achieving an organization's objectives. However, the fact that each component must be present and functioning does not mean that each must function perfectly. Accordingly, monitoring does not seek to conclude on the effectiveness of individual internal control components operating in isolation.

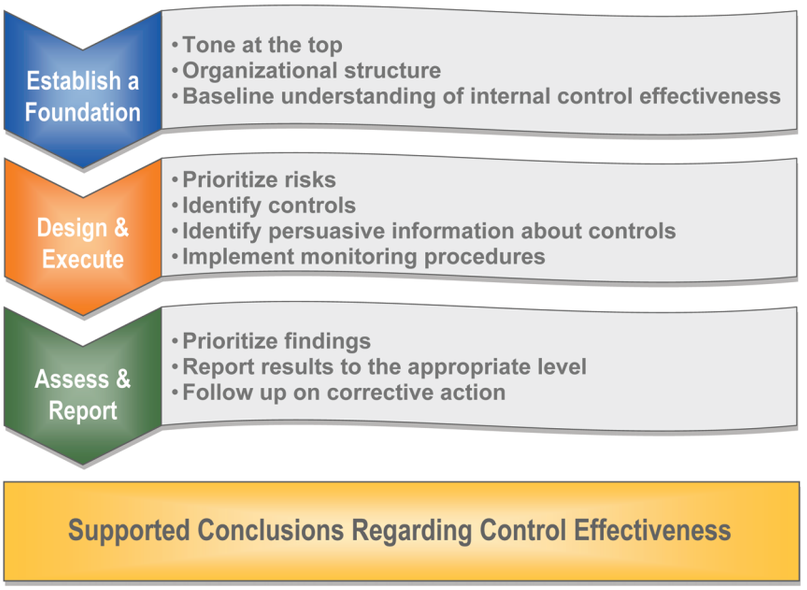


Monitoring Applied to the Internal Control Process
Figure 1

III. A Model for Monitoring

15. An effective approach to monitoring involves (1) establishing a foundation for monitoring, (2) designing and executing monitoring procedures that are prioritized based on risks to achieving organizational objectives, and (3) assessing and reporting the results, including following up on corrective action[8] where necessary (see Figure 2).

See Vol. II, ¶¶ 20–21.



The Monitoring Process
Figure 2

Establish a Foundation for Monitoring

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

See Vol. II, ¶ 22.

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

Tone at the Top

See Vol. II, ¶ 23.

17. 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.

Organizational Structure

See Vol. II, ¶¶ 24–26.

18. *Roles of Management and the Board* — Management has the primary responsibility for the effectiveness of an organization's internal control system. Management establishes the system and implements monitoring to help ensure that it continues to operate effectively. The board's[9] role is one of governance, guidance and oversight. For publicly listed companies, the board's responsibilities may be mandated by law, listing-exchange requirements or charter. For privately held and not-for-profit organizations, the board's responsibilities typically are listed in the board's charter.

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

20. The COSO Framework, on pages 26–27 and 86–87,[10] contains some useful information regarding the role of boards and audit committees that is consistent with this guidance.

See Vol. II, ¶¶ 27–37.

21. *Characteristics of Evaluators* — Monitoring is conducted by evaluators who are appropriately **competent** and **objective**[11] in the given circumstances. Competence

---

[9] Many organizations have boards of directors and related board committees to help oversee the conduct of their activities. Other organizations may not have a formal board of directors, but may have stakeholders who serve in a governance and oversight capacity. For simplicity, this guidance will use the terms "board of directors" or "board" to refer to all groups charged with governance and management oversight.

[10] Competence and objectivity are also relevant factors to consider regarding information sources (i.e., the people responsible for providing monitoring information to evaluators).

[11] Reproduced in Volume II, Appendix B.

refers to the evaluator's knowledge of the internal control system and related processes, including how controls should operate and what constitutes a control deficiency. 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 results for personal benefit or self-preservation.

Baseline Understanding of Internal Control Effectiveness

See Vol. II, ¶¶ 38–41.

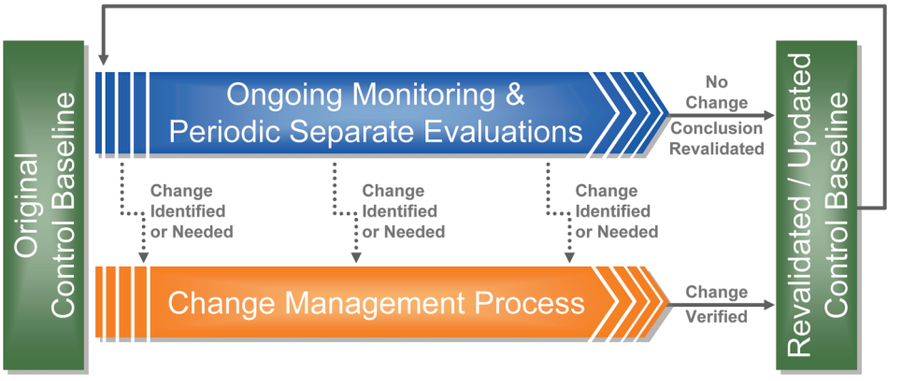
22. Internal control systems fail because:

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

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

- *Control Baseline* — Establishing a starting point that includes 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
- *Change Identification* — Identifying, through ongoing monitoring and separate evaluations, changes in internal control that are either necessary or have already taken place
- *Change Management* — Evaluating the design and implementation of those changes, thus establishing a new baseline
- *Control Revalidation/Update* — Periodically revalidating control operation when no known changes have occurred

24. This broad depiction of monitoring is illustrated in Figure 3. It is intended to demonstrate how monitoring of a known effective internal control system is a process that looks for and evaluates changes that may have a bearing on its effectiveness. It is not intended to dictate monitoring procedures or a documentation format.



Monitoring for Change Continuum
Figure 3

25. Note that the four sequential elements described above in paragraph 23 do not reside solely within the monitoring component. For example, the risk assessment component might be considered chiefly responsible for identifying changes in the operating environment. Likewise, evaluating the proper design and implementation of changes in internal control might be considered a control activity. The monitoring component operates to help ensure that the other components are properly identifying and managing changes that affect internal control.

Design and Execute Monitoring Procedures

See Vol. II, ¶¶ 42–53.

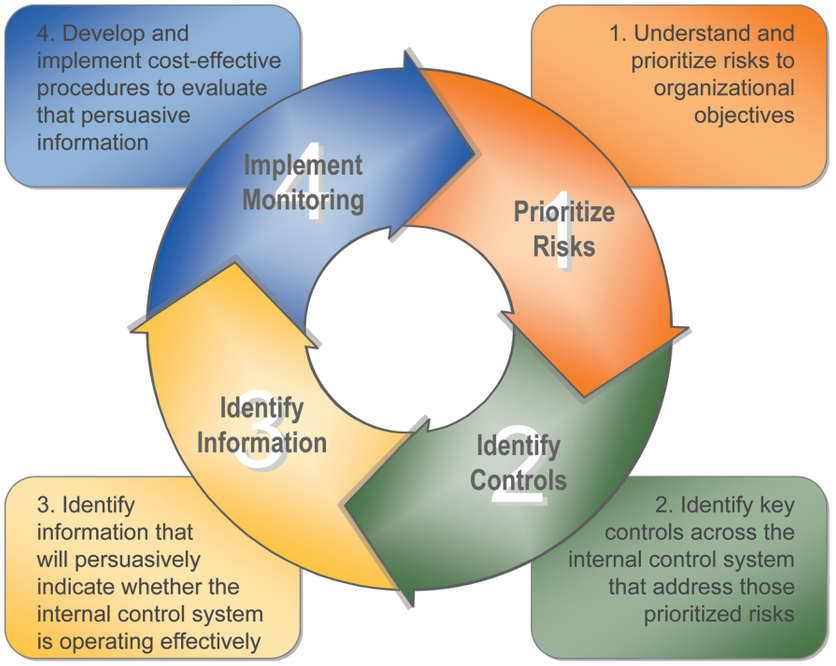
26. Monitoring should enable evaluators to assess **persuasive information** about the operation of one or more controls that address meaningful risks to the organization's objectives. Accordingly, evaluators might consider designing monitoring by following the logical progression depicted in Figure 4. Note, however, that this progression is not meant to imply a rigid, compartmentalized monitoring process where each step starts and stops before the next. Monitoring is a dynamic process and each of these "steps" operates, to some extent, at all times. This graphic, and the discussion that follows, is intended to portray the general flow of monitoring in practice.

See Vol. II, ¶¶ 45–47, 54–58.

1. Prioritize Risks

27. The effectiveness and efficiency of monitoring can be enhanced by linking it to the results of the risk assessment component. This connection enables evaluators to

focus their monitoring attention on controls that address meaningful risks to the organizational objectives for which they are responsible.



Monitoring Design and Implementation Progression

Figure 4

28. Meaningful risks are those that might reasonably, in a given time frame, have a consequential effect on organizational objectives and are determined through the risk assessment component of internal control. Such risks may vary between similar organizations and between different levels within the same organization. For example, controls that mitigate the risk of supplies theft may fall within the monitoring responsibilities of a retail chain store manager, but may not warrant the frequent attention of the chief executive officer in the context of his or her organization-wide responsibilities.

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

See Vol. II, ¶¶ 48–51, 59–62.

2. Identify Key Controls

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

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

32. Organizations can identify key controls[12] by (1) understanding how the internal control system is designed to manage or mitigate meaningful risks, and (2) determining which controls will contribute most to the monitoring conclusion. Key controls often have one or both of the following characteristics:

- Their failure could materially affect the objectives for which the evaluator is responsible, but might not be detected in a timely manner by other controls, and/or
- Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization's objectives.

33. The intent of identifying key controls is not to suggest that some controls are more important to the internal control system than others, but to help organizations devote monitoring resources where they can provide the most value.

See Vol. II, ¶¶ 52, 63–83.

3. Identify Persuasive Information

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

See Vol. II, ¶¶ 63–64.

35. To be effective, monitoring must evaluate a **sufficient** amount of **suitable** information. Suitable information is **relevant**, **reliable** and **timely** in the given circumstances. Sufficient suitable information provides the evaluator with the support needed to conclude on the internal control system's ability to manage or mitigate identified risks. COSO's Monitoring Guidance refers to information that meets these conditions as "persuasive."

---

[12] Key controls can include controls from any of the five COSO components, not just control activities.

36. One important aspect of relevance (and, thus, of persuasive information) is the distinction between **direct** and **indirect information**. Direct information is obtained by observing controls in operation, reperforming them, or otherwise evaluating their operation directly. It 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.

See Vol. II, ¶¶ 65–76.

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

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

39. The value of indirect information in monitoring depends on several factors, including:

- Its level of precision — More-precise indirect information is better able to identify anomalies that indicate a control failure.
- The degree of variability in the outcomes — Indirect information is better able to identify anomalies in processes that typically generate consistent, predictable results.
- The adequacy of the follow-up procedures — The skills and experience of people responsible for investigating anomalies, and the diligence with which they conduct their follow-up procedures, affect the ability of indirect information to identify a control failure.
- The length of time since the operation of the underlying controls was last validated through persuasive direct information — As time passes and operating environments change, indirect information loses its ability to detect control failures. Periodically reestablishing the control baseline using direct information helps evaluators validate or modify the nature, timing and extent of indirect information used in monitoring.

40. The table in Volume II, paragraph 76 highlights some additional factors that may influence an organization's decisions regarding the amount of direct and/or indirect information it uses in monitoring.

See Vol. II, ¶¶ 53, 84–93.

4. Implement Monitoring

41. With risks prioritized, key controls selected, and available persuasive information identified, the organization implements monitoring procedures that evaluate the internal control system's effectiveness in managing or mitigating the identified risks to organizational objectives. 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.

42. The COSO Framework makes an important point with respect to building monitoring into the routine operations of an organization:

> **"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."[13]**

43. Ongoing monitoring occurs when the routine operations of an organization provide feedback — through both direct and indirect information — to those responsible for the effectiveness of the internal control system. It includes regular management and supervisory activities, peer comparisons and trend analysis using internal and external data, reconciliations, and other routine actions. Ongoing monitoring might also include automated tools that electronically evaluate controls and/or transactions.

44. 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. 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 separate evaluations whose sole purpose is to support the external assertions.

45. Separate evaluations can employ the same techniques as ongoing monitoring, but they are designed to evaluate controls periodically and are not ingrained in the routine operations of the organization. They do, however, play an important role in monitoring in that they often:

- Provide an objective analysis of control effectiveness when performed by personnel who are not involved in the operation of the control, and
- Provide periodic feedback regarding the effectiveness of ongoing monitoring procedures.

---

[13] COSO Framework, p. 70.

46. When ongoing monitoring is effective, periodic separate evaluations are used as necessary to reconfirm the conclusions reached through ongoing monitoring. Separate evaluations are also used to address controls that are not subject to ongoing monitoring.

47. As the likelihood and/or potential significance of a control's failure increases, the length of time between separate evaluations typically decreases. Conversely, as risk decreases, organizations may determine to increase the time between separate evaluations. The presence of ongoing monitoring using appropriately persuasive information can also increase the interval between separate evaluations.

Assess and Report Results

48. Monitoring includes reporting results to appropriate personnel. This final stage enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control or highlight identified deficiencies for possible corrective action.

See Vol. II, ¶¶ 94–95.

Prioritize and Communicate Results

49. Identifying and prioritizing potential control deficiencies allows organizations to determine (1) the levels to which the potential deficiencies should be reported, and (2) the corrective action, if any, that should be taken. Several factors may influence an organization's prioritization of identified deficiencies, including:

See Vol. II, ¶¶ 96–97.

- The likelihood that the deficiency will materially affect the achievement of an organizational objective,
- The effectiveness of **compensating controls**, and
- The aggregating effect of multiple deficiencies.

Report Internally

See Vol. II, ¶¶ 98–101.

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

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

Reporting in such cases might be limited to local management personnel for whom the local goals are relevant.

52. 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.

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

See Vol. II, ¶¶ 102–107.

Report Externally

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

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

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

- Using evaluators with a higher degree of objectivity in certain areas if doing so will enhance the ability of the external party to use their work;

- Increasing the use of direct information in monitoring of certain areas if doing so will enable the external party to more effectively and efficiently support its own conclusions; and
- Increasing the formality and detail of documentation in order to improve the external party's ability to understand and evaluate internal control.

57. Most external reporting requirements are developed to address risks that are already contemplated by properly designed and executed monitoring procedures. 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.

See Vol. II, ¶¶ 105–107.

Other Considerations

Monitoring Controls Outsourced to Others

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

See Vol. II, ¶¶ 108–109.

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

See Vol. II, ¶¶ 110–114.

Using Technology for Monitoring

60. Organizations often use information technology (IT) — through control monitoring tools and process management tools — to enhance monitoring. As the use of IT increases, both as part of an organization's operations and as tools used in monitoring, the need increases to evaluate internal control over those information systems.[14]

61. *Control Monitoring Tools* — Automated control monitoring tools perform routine tests and can enhance the effectiveness, efficiency and timeliness of monitoring specific controls. Some control monitoring tools are used to perform what is often referred to as "continuous controls monitoring." These tools complement normal transaction processing by checking every transaction, or selected transactions, for the presence of certain anomalies (e.g., identifying transactions that exceed certain thresholds, analyzing data against predefined criteria to detect potential controls issues such as duplicate payments, or electronically identifying segregation of duties issues). Many of these tools serve more as highly effective control activities (detecting individual errors and targeting them for correction before they become material) than they do as internal control monitoring activities. Regardless, if they operate with enough precision to prevent or 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.

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

See Vol. II, ¶¶ 115–118.

Formality and Level of Documentation

63. 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

[14] See Volume III, Chapter VI for more detailed application techniques regarding the use of technology in monitoring.

the senior-management and board levels, thus increasing the need for more-formal monitoring documentation.

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

65. 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.

Scalability of Monitoring

66. 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.

67. *Scalability Based on Size* — 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, both bodies 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 (all of which "roll up" to a home office or headquarters). The ongoing monitoring activities typically are augmented by separate evaluations that are performed by a qualified internal audit function or other parties (e.g., lower-level management or other departments) and which lend support to the conclusion that the lower-level monitoring systems are operating effectively.

See Vol. II, ¶¶ 120–123.

68. In smaller organizations, on the other hand, monitoring at the senior-management level often occurs much closer to the risk and related controls, giving the evaluators more direct information about the operation of controls. The greater quantity of direct information about the operation of internal control may allow the evaluator in a smaller organization to support his or her control conclusions without adding the additional monitoring procedures that may be necessary in a larger organization where the evaluator is further removed from the operation of controls.

69. *Scalability Based on Complexity* — Size notwithstanding, some organizations are more complex than others. Factors influencing complexity include industry characteristics, regulatory requirements, number of products or service lines, level of centralization versus decentralization, use of prepackaged versus customized

See Vol. II, ¶¶ 124–127.

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

70. Because the level of complexity may vary by department or area, scaling of monitoring based on complexity is more difficult to apply to an entire organization than is scaling based on size. For example, an organization may use a prepackaged information system for one of its business processes, which can reduce certain IT-related risks (such as the risk of incorrect programming), but that same organization might also use a complex, internally developed software system for another business process, which, unless well controlled, can increase IT-related risks.

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

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

IV. Summary Considerations

73. Properly designed and executed monitoring (1) provides persuasive information to evaluators regarding the internal control system's effectiveness, and (2) identifies and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate. In doing so, it facilitates the correction of control deficiencies *before* they materially affect the achievement of the organization's objectives.

74. The following general principles may be helpful in determining how best to utilize COSO's Monitoring Guidance:

1. Organizations should follow a systematic process in determining "what" and "how" to monitor. Figure 2 portrays such a process.
2. Monitoring considers how the entire internal control system addresses meaningful risks, not how individual control activities operate in isolation.
3. The board has important oversight responsibilities in monitoring internal control (especially the controls that relate to ensuring a strong tone at the top) and in mitigating the risk of management override.
4. A baseline understanding of internal control design and operating effectiveness serves as a good starting point for implementing monitoring procedures that are both effective and efficient.

5. Determining *what* to monitor should be influenced by:
    a. The significance and likelihood of the underlying risk,
    b. The nature of the controls that are designed to address the risk, and
    c. The persuasiveness of the information needed to conclude whether the identified controls are operating effectively.
6. Organizations should consider using ongoing monitoring, when feasible, over separate evaluations where the risks and availability of information merit such an approach.
7. Effective monitoring relies on the development of *persuasive information* about the continued operation of controls or control elements, as evaluated by appropriately *competent and objective* evaluators.
8. Management must be enabled and expected to exercise reasonable judgment in determining the optimal approach to monitoring.
9. Monitoring generally includes the use of both direct and indirect information. However, indirect information can be used only for a finite period of time without some direct information supporting a conclusion that the underlying control is operating effectively.
10. Identified control deficiencies should be:
    a. Evaluated as to their severity,
    b. Reported to appropriate personnel, and
    c. Considered for corrective action.

75. In addition to the considerations above, organizations may benefit from periodically evaluating the overall effectiveness and efficiency of monitoring. The following questions — which may be asked at various levels, including the board level — may help with regard to those evaluations.

See Vol. II, ¶¶ 128–129.

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

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