Monitoring of Internal Controls and IT

A Primer for Business Executives, Managers and Auditors on How to Advance Best Practices

EXPOSURE DRAFT

25 March 2010

Guidance

Key Principles

Best Practices

ISACA®

Trust in, and value from, information systems

ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA® (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA offers the Business Model for Information Security (BMIS) and the IT Assurance Framework (ITAF). It also developed and maintains the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

Disclaimer

ISACA has designed and created *Monitoring of Internal Controls and IT* exposure draft (the "Work") primarily as an educational resource for business executives, managers and auditors. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information procedures and tests or exclusive of other information procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information procedure or test, readers should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Monitoring of Internal Controls and IT Exposure Draft

Acknowledgments

ISACA wishes to recognize:

Development Team

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Everett C. Johnson Jr., CPA, Deloitte LLP (retired), USA, Assistant Chair
Christopher Fox, ACA, CA Inc., USA
Mike Garber, CGEIT, CIA, CPA, Motorola Inc. (retired), USA
J. Russell Gates, DuPage Consulting, USA
Elsa K. Lee, CISA, CISM, CGEIT, CSQA, AdvanSoft International Inc., USA
Steve Reznik, CISA, The ALS Group, USA
Robert Soles, CISA, CPA, KPMG LLP, USA

Expert Reviewers

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Everett C. Johnson Jr., CPA, Deloitte LLP (retired), USA, Assistant Chair
Mark Adler, CISA, CISM, CGEIT, Commercial Metals Company, USA
Brian Barnier, CGEIT, ValueBridge Advisors, USA
Gerard (Rod) Brenan, Ph.D., Siemens Corp., USA
Akhilesh Chandra, Ph.D., CGEIT, ACS, University of Akron, USA
Kim Coleman, CISA, ING North American Insurance Corp., USA
Mike Garber, CGEIT, CIA, CPA, Motorola Inc. (retired), USA
J. Russell Gates, DuPage Consulting, USA
Robert D. Johnson, CISA, CISM, CGEIT, CISSP, ING US Financial Services, USA
Elsa K. Lee, CISA, CISM, CGEIT, CSQA, AdvanSoft International Inc., USA
Philip M. LeGrand, UK
Leanne McRill, CISA, CPA, USA
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Beth Pumo, CISA, CISM, University of Michigan Health System, USA
Sridhar Ramamoorti, Ph.D., ACA, CFE, CFFA, CFSA, CGAP, CGFM, CIA, CICA, CPA/CITP/CFF, CRP, FCPA, Infogix, Inc., USA
Steve Reznik, CISA, The ALS Group, USA
Scott Shinners, CISA, CPA, ConAgra Foods Inc., USA
Robert Soles, CISA, CPA, KPMG LLP, USA
Timothy J. Van Ryzin, CISA, CISM, Harley-Davidson, USA
Miklos A. Vasarhelyi, Ph.D., Rutgers Business School, USA
Mark Zanaglio, CGEIT, AMA, PMP, Wachovia, USA

Focus Group

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Everett C. Johnson Jr., CPA, Deloitte LLP (retired), USA, Assistant Chair
Mark Adler, CISA, CISM, CGEIT, Commercial Metals Company, USA
Akhilesh Chandra, Ph.D., CGEIT, ACS, University of Akron, USA
Christopher Fox, ACA, CA Inc., USA
Mike Garber, CGEIT, CIA, CPA, Motorola Inc. (retired), USA

John Hainaut, Jefferson Wells, USA
Hussain Hasan, CISM, CGEIT, CISSP, RSM McGladrey, Inc. USA
Jan Hertzberg, CISA, CISSP, Grant Thornton LLP, USA
Phil Lageschulte, CPA, KPMG LLP, USA
Elsa K. Lee, CISA, CISM, CGEIT, CSQA, AdvanSoft International Inc., USA
David Matheson, CISA, Zurich North America, USA
Dave McKeon, CISA, Deloitte LLP, USA
Leanne McRill, CISA, CPA, USA
Joseph J. Nocera, PricewaterhouseCooper LLP, USA
Cory Notrica, CISA, CISM, CGEIT, Pepsico, USA
John G. Ott, CISA, CPA, AmerisourceBergen, USA
Sridhar Ramamoorti, Ph.D., ACA, CFE, CFFA, CFSA, CGAP, CGFM, CIA, CICA, CPA/CITP/CFF, CRP, FCPA, Infogix, Inc., USA
Steve Reznik, CISA, The ALS Group, USA
Ken Schmidt, CISA, CISSP, CPA, The Options Clearing Corporation, USA
Scott Shinners, CISA, CPA, ConAgra Foods Inc., USA
Robert Soles, CISA, CPA, KPMG LLP, USA
Doug Underwood, McGladrey & Puillen, USA
Don Warren, Rutgers University, USA

Guidance and Practices Committee

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair
Phillip J. Langeschulte, CGEIT, CPA, KPMG LLP, USA
Mark A. Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Adel H. Melek, CISA, CISM, CGEIT, Deloitte & Touche, Canada
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Private Ltd, India
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Salamon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Eddy Schuermans, CISA, CGEIT, ESRAS bv ba, Belgium
Frank Van Der Zwaag, CISA, CISSP, Westpac, New Zealand

Three days have passed.

Your teams still cannot process customer transactions. It looks like a minor change to a critical computer application crashed a key revenue-supporting system.

Your top people are on it. And you should be back in business by 6:00 a.m. tomorrow.
But as the CEO of a global enterprise with billions in revenue, this is an unpleasant surprise.

After all, just last year you put in multiple program change controls—and a whole range of key measures. Like business approval. And documented test results.

Your chief risk officer calls. Apparently, your controls have degraded over the last 14 months. Proper monitoring, some of it automated—along with better access to what your risk and compliance experts formally refer to as “persuasive information”—would have detected the degradation.

And prevented the business crisis.

Preventing this from occurring again is about explicitly acknowledging the critical role that monitoring can play—particularly with respect to the monitoring of IT controls—and the automation of some key monitoring processes.

There is an established body of knowledge on this crucial process and a well-defined set of good practices.

You just need to apply them.

Table of Contents

1. Overview of the Use of Internal Controls and Monitoring

Now that internal controls are finally, on the whole, embedded in the critical business processes that drive enterprise success, the strategic spotlight has shifted.

Where? To monitoring.

Since passage of laws such as the 1977 US Foreign Corrupt Practices Act, which required enterprises to implement internal control programs, and in the 20 years since the formation of COSO,[1] there has been an enormous increase—a sea change—in the number of enterprises with an established, documented set of internal controls firmly in place.

The Value of Internal Controls Is Beginning to be Acknowledged

By itself, this is not surprising. After all, across global business markets and jurisdictions from Asia to Europe and the Americas, the number of regulations has skyrocketed. Boards have increased their compliance focus. How well executives manage risks to performance at every level of the enterprise, from critical business processes to individual business units and the enterprise as a whole, can have enormous impacts ranging from defining market leadership for the enterprise to bringing careers to an abrupt halt.

Management's stewardship of resources requires effective governance, adequate controls to protect the resources, and a monitoring process that alerts management to changes in the business and control processes in a timely manner.

Just having these elements in place, however, is not enough even if they extend well beyond the financial controls required by regulations, such as the US Sarbanes Oxley Act, to the operational controls used to guide a much broader range of critical business processes, transactions and systems.

Why? Control effectiveness degrades over time.

Breakdowns occur. Sometimes internal controls do not operate as designed. They fail to keep up with the business and their alignment with strategic objectives or changing operational constraints. Perhaps key controls are missing or the enterprise lacks processes to design, implement, enforce, communicate or revise them.

The Strategic Importance of Effective Monitoring

One credible and trustworthy means of ensuring the effectiveness of internal controls and countering the risks of this degradation and breakdown is to monitor them.

[1] Committee of Sponsoring Organizations (COSO) of the Treadway Commission was formed in 1985, *www.coso.org*.

Ensuring the integrity, discipline and effectiveness of their control activities, information collection and communication processes, and overall control environment is currently one of the most common, potentially critical and frequently overlooked challenges facing executives responsible for governance, risk management, compliance and internal audit.

One of the biggest obstacles to the effective monitoring of an enterprise's control structure is the ability to obtain economical and reliable feedback on a control's strategic effectiveness and reliability. To overcome this obstacle, management often can leverage technology to devise a sustainable process that can operate seamlessly within the normal operational infrastructure.

Technology's Role in Monitoring

Technology can be important to the monitoring of internal controls in two related but very different ways. It is both an enabler of effective monitoring and, as an important part of many internal controls, a key area that must be monitored in its own right.

Currently, technologies provide management with the opportunity to improve monitoring and oversight of business processes and controls. For example, the growth and complexity of enterprise resource planning (ERP) systems, the increased use of networks and speed of processing, and the globalization of business have driven the development of more intelligent software tools. These tools can now help management to better capture and analyze key data for strategic and operational decisions and trigger alarms when unusual transactions or patterns occur.

Apart from enabling monitoring, technology is often an integral supporting component for internal controls and must itself be subjected to rigorous oversight. For instance, technology-based systems—many of them automated—are often the source of information used by auditors and risk managers to answer two critical questions: what to monitor and how to monitor it. Inaccurate or incomplete information can lead to a breakdown in governance and misguided risk management strategies and outcomes.

To provide executives with faster access to quality data on the efficiency and effectiveness of enterprise risk management activities, monitoring of internal controls must reach beyond financial reporting risks.

To what?

To operational and compliance risks—such as achieving business strategies, containing cost, meeting regulatory requirements, and protecting the privacy of personal information.

The monitoring of information technology (IT) controls and automation of the monitoring process can offer substantial benefits. These include:

- Earlier identification and timely corrective action of breakdowns in processes and internal control deficiencies
- Leveraging of processes to monitor controls to also monitor business performance. Information used for one can be used for the other and vice versa. Emphasizing to boards the value add of monitoring business performance and early warning systems is often the best way to justify the investment in monitoring tools and technology.
- Provision of more accurate, decision-relevant information through reliable financial and operational reporting
- Better access to real-time data and, by extension, increased speed and quality of management decision making
- Enhanced assurance of compliance with laws and regulations
- Ability to furnish periodic certifications or assertions on the effectiveness of the framework of internal controls
- Better detection and prevention of fraud, waste and abuse, and reduced business impact when they do occur
- Removal of excess costs from operations through more efficient controls and processes
- Increased management confidence in the information generated by business processes

Timely Feedback: The Virtues of Automation

Automated monitoring processes have significant advantages. They are replicable, consistent and can handle huge volumes of transactions and data at great speed.

This can significantly increase efficiency and decrease the cost of operations. When many key systems and control processes within an enterprise rely on information technology, the most effective way to perform monitoring is to automate the monitoring process. In some situations, it is neither cost-effective nor desirable to monitor automated processes and controls without using IT.

Here is an example. While the review of security controls on one server can be achieved by reviewing the security settings directly, this may not be feasible in large or geographically dispersed enterprises as there may be too many servers in too many places. It may be necessary to automate the monitoring processes by downloading the security settings from the servers and comparing them to the enterprise standard. When the security settings are different, the enterprise can determine whether the appropriate controls were followed to authorize the exception. This type of approach provides relevant, reliable and timely information for monitoring in an efficient and effective manner.

Automated monitoring processes can be particularly effective when information about controls is dispersed or voluminous, or to address conditions that drive fraud and waste.

How Automating Internal Controls Monitoring Can Reduce Fraud

Fraud is more likely when basic internal control processes are ineffective, can easily be circumvented, or changes in employee responsibilities result in a lack of segregation of duties. An effective monitoring approach, especially when it is automated, may serve as a deterrent to potential fraud. Employees may be more reluctant to attempt a defalcation when they are aware that management has a process in place to monitor their activities.

One common practice, continuous controls monitoring, complements normal transaction processing by checking every transaction or selected transactions against pre-specified criteria (e.g., identifying transactions that exceed pre-defined thresholds or flagging transactions with segregation of duties conflicts).

Monitoring often occurs at several levels of management. The most important monitoring procedures are likely to be monitored by senior management to ensure that they are performed effectively by operational management. In such cases, the monitoring activity performed by operational management may be treated like a key control from a senior management point of view.

How to Use This Publication

The purpose of this publication is to provide useful guidance and tools for enterprises interested in applying information technology to support and sustain the monitoring of internal control. In addition, this document provides practical guidance for the design and operation of monitoring activities over existing IT controls. Effective IT-enabled monitoring can be of benefit to senior management, which includes the governance bodies, the audit committee and the board of directors. However, management should carefully consider the monitoring mechanisms that are appropriate and necessary for its own circumstances. Management may choose not to include all of the activities and approaches discussed in this document, and, similarly, may choose activities not discussed in this document. In either case, it is expected that customization of the approaches provided in this document will be necessary to reflect the specific circumstances of each enterprise.

This publication is intended to assist in this regard, primarily using relevant COSO and COBIT content. Appendix A discusses monitoring of internal controls and IT, and integration with COBIT, Val IT and Risk IT.[2]

[2] COBIT, Val IT and Risk IT are frameworks developed and maintained by ISACA, *www.isaca.org*.

2. Foundational Concepts and Principles of Monitoring

It is very important to understand the "building blocks" of an effective monitoring capability.

One reason, among many, is that addressing the failure of controls early costs a lot less than remediating and redesigning key monitoring processes later.

Let us first establish the "ground rules" or, more accurately, the broader background concepts, principles and considerations that help structure a consistent and uniform approach to:

- Design and execute a monitoring process (chapter 3)
- Automate controls monitoring to increase efficiency and effectiveness (chapter 4)
- Address other important considerations (chapter 5)

A Key Starting Point: COSO's Guidance on Monitoring

What exactly is "monitoring" and what makes it "effective"?

Figure 1—COSO Framework

Monitoring, according to COSO's 1992 *Internal Control—Integrated Framework*, is the set of tasks implemented to help ensure that internal controls continue to operate effectively. The COSO Framework consists of five interrelated and equally important components, depicted in **figure 1**. COSO's 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*, and COSO's 2009 *Guidance on Monitoring Internal Control Systems* enhanced the understanding of monitoring by articulating the following two related principles:

- *Ongoing monitoring* and/or *separate evaluations* enable management to determine whether the other components of internal control 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.

In January 2009 COSO issued its *Guidance on Monitoring Internal Control Systems*. This monitoring guidance consists of three volumes: Volume I provides general guidance, Volume II provides application guidance, and Volume III contains illustrative examples. Although using the guidance contained in this publication does not require the reader to have read the COSO guidance, it would be beneficial to most individuals to read the COSO guidance as it provides additional background and perspective on many of the concepts presented herein.

In Volume II of its monitoring guidance, COSO states that in an effective internal control system, the COSO Framework's five components work together, providing reasonable assurance to management and the board of directors regarding the achievement of the enterprise's objectives. The monitoring component helps ensure that the internal control system continues to operate effectively. As such, the effective operation of the monitoring component provides value to the enterprise in three ways:

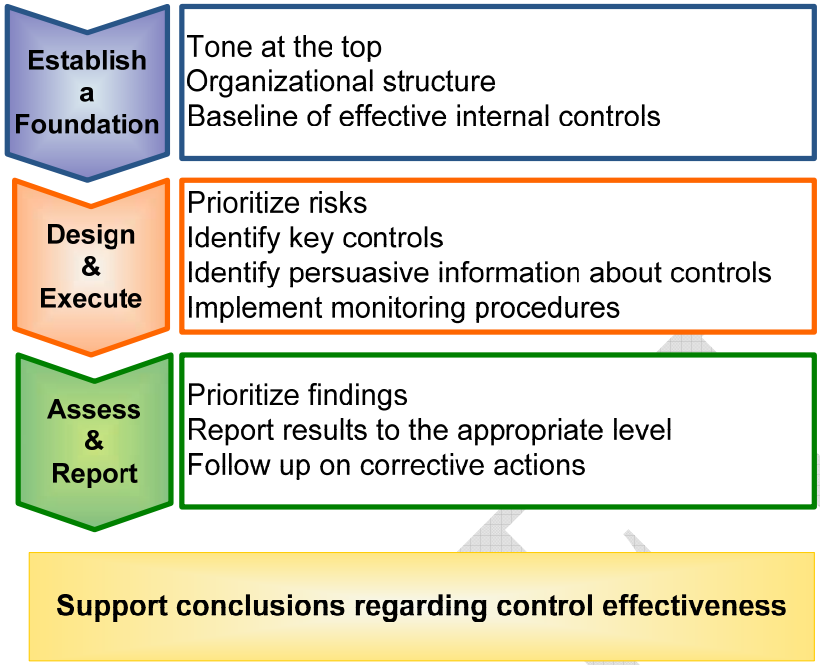
- It enables management and the board to determine whether the internal control system, including all five components, continues to operate effectively over time. Thus, it provides valuable support for assertions, if required, about the internal control system's effectiveness.
- It improves the enterprise's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

COSO goes on to say that effective monitoring is based on three broad elements:

1. Establishing a foundation for monitoring, including a proper tone at the top; an effective organizational structure; and a starting point or "baseline" of known, well-designed and -implemented controls
2. Designing and executing monitoring procedures focused on *persuasive information* about the operation of key controls that address meaningful risks to organizational objectives
3. Assessing and reporting results, which include evaluating the severity of any identified deficiencies and reporting the monitoring results to appropriate parties to enable timely corrective action

COSO further illustrated these elements in its Model for Monitoring, depicted in **figure 2**.

Figure 2—COSO Model for Monitoring



Each one of these elements is important in supporting this model; however, examining persuasive information is an ideal one with which to begin, as it is such a foundational key requirement for effective monitoring.

Information: A Requirement for Monitoring

In many respects, information is a requirement, not just for internal controls, but also, and just as importantly, for an effective monitoring program. In fact, within the field of internal control and monitoring, specific meanings apply to a wide range of terms for types of information such as “persuasive information,” “suitable information” and “sufficient information,” among other terms. Here is a brief overview of these terms.

Persuasive Information

Persuasive information provides adequate support for a conclusion regarding the effectiveness of internal control. Persuasive information is both *suitable* and *sufficient* in the circumstances and gives the person responsible for verifying that a control is operating (the evaluator) reasonable, but not necessarily absolute, support for a conclusion regarding continued effectiveness of the internal controls. An appropriate cost-benefit analysis—one that weighs the effort to gather the information against the ability of the information to persuade the evaluator a control process continues to operate effectively—is an important part of effective, sustainable monitoring activity. This analysis is normally qualitative in nature, but may contain quantitative measurements as well. Regardless of the method, those

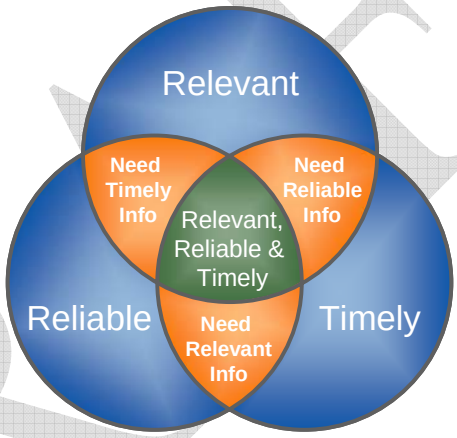
responsible for monitoring must exercise judgment in determining the information necessary to have reasonable, but not necessarily absolute, support for a conclusion regarding continued control effectiveness in a given area.

Suitable Information

Suitable information is a broad concept that implies that information is useful within the context for which it is intended. To be suitable, information must be *relevant*, *reliable* and *timely*.

Figure 3 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/her attention to whether sufficient information is available to form a reasonable conclusion.

Figure 3—Elements of Suitable Information



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.

- **Relevance of information**—Information is relevant when it tells the evaluator something meaningful about the operation of the underlying controls. When evaluators obtain relevant information about control effectiveness, they identify characteristics or attributes indicative of the control's proper performance or failure. They can then test for the presence or absence of these conditions using persuasive direct and indirect information (two additional terms that are discussed in following sections). Information that directly confirms the operation of controls is more relevant than information that requires a greater degree of inference to conclude whether the controls are effective.
- **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 a

prerequisite to reaching correct conclusions. Verifiable information enables evaluators to know whether the information can be trusted. 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.

- **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 significant. Suitable information must also relate to the period under consideration. As information ages, it loses its ability to tell the evaluator whether the related controls are operating properly. Likewise, information produced after a control operates may not help support earlier point-in-time conclusions.

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 3**, additional information is needed to achieve the required degree of suitability. Determining the suitability of information being used is a matter of judgment.

Sufficient Information

Sufficiency is a measure of the quantity of information (i.e., whether the evaluator has enough suitable information). Evaluators must gather sufficient suitable information to support a reasonable conclusion about control effectiveness. Sufficiency can refer to how many occurrences of a given process or control are evaluated (e.g., 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. Regardless, the evaluator must exercise judgment in determining whether he/she is evaluating enough information.

Direct and Indirect Information

Direct information substantiates the operation of controls and business process performance. It is obtained by observing controls in operation, and reperforming them or otherwise evaluating their operation directly, and can be useful in both ongoing monitoring and separate evaluations (discussed in a following section). Generally, direct information is highly relevant because it provides an unobstructed view of control operation.

Indirect information provides a context within which the direct information may be properly evaluated. It may include all other information that *may* indicate a change or failure in the operation of controls. It either relates to or is produced by the process in which the controls reside. Indirect information often can be used to

monitor both controls and business processes. Indirect information can include, but is not limited to:

- Operating statistics
- Key risk indicators
- Key performance indicators
- Comparative industry metrics

Monitoring using indirect information identifies anomalies that may signal a control change or failure and subjects that control to investigation. Since indirect information does not, however, provide an unobstructed view of control operation, 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 anomalies, or the indirect information may have lost its ability over time to identify anomalies. Indirect information is thus limited as to the level of support (i.e., persuasiveness) it can provide on its own, especially over a long period of time.

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

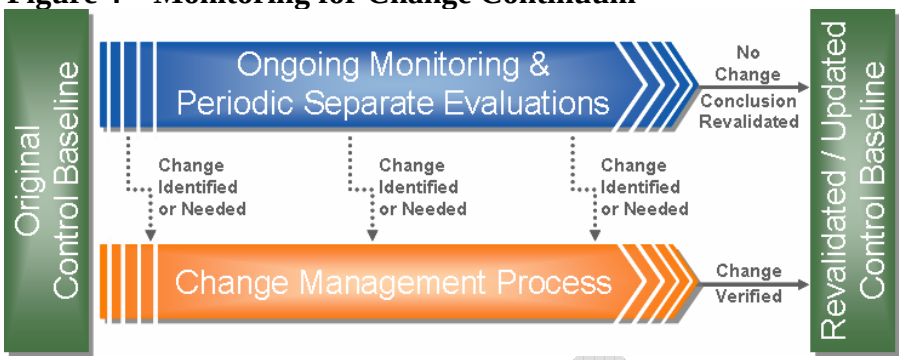
- Signal that a change in the environment or control operation has occurred
- Supplement the support provided by direct information—sometimes for an extended time frame—regarding the evaluator's conclusions about control effectiveness

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

The Importance of Establishing a Control Baseline

The concept of benchmarking (also known as a control baseline) was included in COSO's *Enterprise Risk Management—Integrated Framework* in 2004 and was discussed in appendix D of *IT Control Objectives for Sarbanes-Oxley, 2nd Edition,* published by ISACA in 2006. The idea of benchmarking can also be applied to monitoring. Establishing a control baseline in a given area can serve as an appropriate starting point for monitoring. Such a baseline allows enterprises to design their monitoring procedures (ongoing and separate evaluations) in a way that usually allows for greater efficiency, as shown in **figure 4**. The baseline provides a benchmark against which ongoing monitoring and separate evaluations can be measured. Deviations from the baseline include changes in the controls themselves (e.g., new personnel perform the control in a different manner) or changes due to control degradation or failure, which trigger the change management process to arrive at an updated baseline.

Figure 4—Monitoring for Change Continuum



The Difference Between Ongoing Monitoring and Separate Evaluations

Ongoing monitoring comprises the set of activities necessary 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.

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

One subset of ongoing monitoring is continuous monitoring; an automated mechanism that provides real-time feedback for management to ensure that systems and controls have been operating as designed and transactions are processed appropriately. For purposes of this discussion, “continuous” is viewed as the normal operating frequency of the key control being monitored. For example, if the key control operates on a weekly basis, then executing the monitoring activity weekly would be considered continuous.

Separate evaluations can employ the same techniques as ongoing monitoring, but they are designed to evaluate controls *periodically* and are not embedded in the routine operations of the enterprise. When separate evaluations are performed by people who are not involved in the operation of the business process or the controls being monitored, they may provide a more objective analysis of control effectiveness than when these evaluations are performed by personnel who are directly involved. As such, they may provide a more objective analysis of control effectiveness than ongoing monitoring procedures that often are performed by less

objective personnel. Separate evaluations can also provide valuable periodic feedback regarding the effectiveness of ongoing monitoring procedures, particularly if the ongoing monitoring is based only on indirect information.

COSO's 2006 guidance *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* addresses the role of ongoing monitoring and separate evaluations and includes the following helpful attributes of each:

- **Integrates with operations**—Ongoing monitoring is built into the enterprise's routine operating activities.
- **Provides objective assessments**—Ongoing monitoring and/or separate evaluations provide an objective consideration of effectiveness.
- **Uses knowledgeable personnel**—Evaluators understand the components being evaluated and how those components relate to activities supporting the enterprise's objectives.
- **Considers feedback**—Management and the board receive feedback on the effectiveness of business performance and internal control.
- **Adjusts scope and frequency**—Management varies the scope and frequency of separate evaluations depending on the significance of processes and risks being controlled, the nature of monitoring processes and the effectiveness of ongoing monitoring, particularly if the ongoing monitoring is based on indirect information only.

The concepts of ongoing monitoring and separate evaluations are further discussed in chapter 5.

Six Key Monitoring Considerations

As an introduction to the next three chapters, it may be helpful to discuss the following six fundamental considerations regarding monitoring and IT. These are first listed and then discussed in greater detail. (Case examples that illustrate the application of the IT considerations are included in appendix B.)

The six key considerations are:

1. Key controls that are IT dependent usually are dependent on selected IT general controls.
2. The risk assessment process and the availability of computerized information drive which IT and manual controls will be monitored.
3. Information needed for monitoring may be available only from an IT process.
4. Monitoring of IT controls and automated monitoring often can be leveraged to address multiple monitoring objectives.
5. When key controls are IT dependent, underlying IT general controls need to be monitored.
6. IT facilitates a repetitive, and often a continuous, monitoring process.

Consideration 1: Key controls that are IT dependent are usually dependent on selected IT general controls.

When a key control is performed by an IT application or uses information produced by an IT application, such a control is usually dependent on one or more IT general controls.

Example of Consideration 1

An exception report produced by an IT application is dependent on effective controls over the development of and changes to that application, particularly those procedures related to ensuring that the exception reporting function is properly tested and changed only as authorized. In addition to monitoring management's follow-up on the exceptions reported, consideration also should be given to monitoring the IT general controls over development of and changes to that application that are important to ensuring that the exception reporting process is effective.

Consideration 2: The risk assessment process and the availability of computerized information drive which IT and manual controls will be monitored.

Designing a monitoring approach begins with understanding and prioritizing the risks to achieving important organizational objectives. Prioritizing risks helps identify which risks are meaningful enough to be subjected to control monitoring. The most important controls (i.e., key controls) are selected for monitoring. In many situations, these key controls are performed by an IT application or are performed manually using information or reports produced by an IT application. In addition, some of the more important risks identified may be IT-related, which would frequently result in a higher priority for monitoring the IT controls related to such risks. When IT controls are selected for monitoring, the availability of computerized direct or indirect information should be considered as it would facilitate the automation of monitoring.

Example of Consideration 2

In an online banking application there is a risk that unauthorized individuals may gain access to cash or investment accounts and make inappropriate transfers of funds. In this situation, the key controls selected for monitoring might include IT application security controls over access to such accounts and the IT general controls related to security. In addition, there may be IT application controls designed to detect such unauthorized transactions, which could be monitored.

Consideration 3: Information needed for monitoring may be available only from an IT process.

Frequently, direct information for monitoring may be available only from an IT process. Additionally, that direct information may not be available from the basic functionality already built into an enterprise's application systems, but may require additional functionality built into or bolted onto existing systems. Direct information is more relevant than indirect information to the operation of the

controls. When direct information can be used, the monitoring procedures will be more effective. In some cases, this information can be used to automate the monitoring process, which can further improve its effectiveness and efficiency.

Example of Consideration 3

Direct information may include a report of changes to a pricing file indicating the business risk of the change and the names of the individuals making and approving the change. This report can be used for monitoring that all master file changes are for appropriate business reasons and are properly approved.

Consideration 4: Monitoring of IT controls and automated monitoring often can be leveraged to address multiple monitoring objectives.

IT general controls are usually part of a common process that affects multiple IT applications. Therefore, if certain IT general controls are selected as key controls for monitoring, the benefits of the monitoring process can be leveraged over all IT applications that are subject to that common process. Similarly, if the monitoring of such IT controls can be automated, the related benefits can be leveraged over all of the related IT applications.

Example of Consideration 4

Monitoring of general controls over security and access to systems and information ordinarily will provide assurance about most, if not all, applications processed by IT. Monitoring this control can be particularly important where authorization to execute transactions is performed through the system or where segregation of duties is important. Similarly, monitoring of controls over system development and changes can provide assurance regarding the proper and consistent functioning of all IT applications subject to the development and change control process.

Consideration 5: When key controls are IT-dependent, underlying IT general controls need to be monitored.

Many IT applications include automated controls to prevent entering or processing invalid transactions or to flag them for timely follow-up before they can be processed further. If such controls are selected as key controls, consideration should be given to monitoring relevant IT controls that provide assurance about the effectiveness of such preventive or detective controls.

Example of Consideration 5

A key control in a sales order system prevents processing a sales order for a new customer until the credit manager has entered an indication that the customer's credit has been checked. A related IT control for monitoring is the access control that ensures that only the credit manager can enter the credit check indication into the system.

Consideration 6: IT facilitates a repetitive, and often a continuous, monitoring process.

When a key control is performed by IT, the monitoring procedures for such a control frequently can be automated and performed on a repetitive periodic or even a continuous basis.

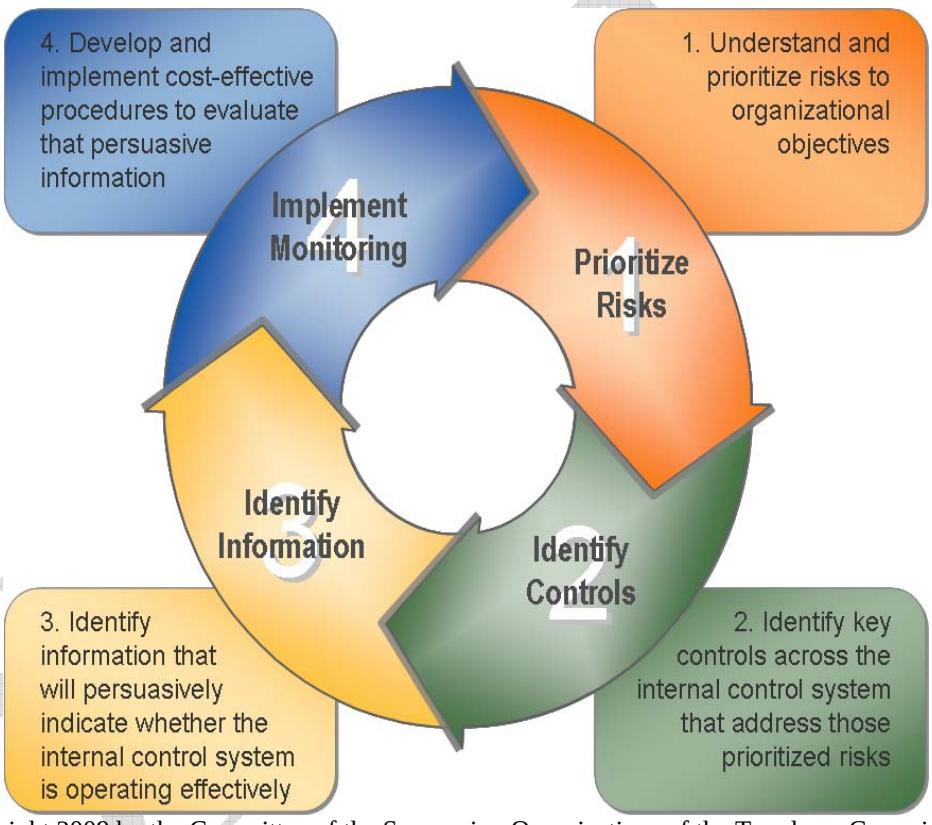
Example of Consideration 6

A key IT general control is that the business unit manager responsible for IT applications approves all changes to the unit's applications. When a change is made to an application, the IT system automatically sends a report to the relevant business unit manager the next day. This allows the business unit manager to ensure, on a timely repetitive basis, that the changes were previously approved or to approve any changes that were made on an emergency basis.

3. How to Design and Execute an IT Monitoring Process

This chapter is a guide to designing and executing a risk-based monitoring program for key IT-related controls. In its 2009 guidance, COSO outlined a four-step process that can be used for designing and executing an effective monitoring process, shown in **figure 5**.

Figure 5—Four-step Process to Design an Effective Monitoring Process



Each of these four steps will be discussed with a specific focus on IT implications and on how IT solutions can be used to monitor certain types of controls. Readers of this document may also want to familiarize themselves with the overall COSO internal control framework and specifically the content in chapter 3 of Volume II of the COSO 2009 guidance for a complete understanding of each of the steps.

In considering the steps in **figure 5**, it is important to consider the following:

- Although depicted in a sequential fashion, this is not meant to depict a rigid process. Monitoring is a dynamic process and each of these "steps" is potentially being performed to some extent in various parts of an organization at different times. For example, the identification of risks and key controls is

frequently an interactive, not sequential, process.

- The first two steps in **figure 5** are derived from the risk assessment and control activities components of the COSO internal control framework. The steps do not imply that these activities need to be reperformed as a discrete part of an effectively implemented monitoring program. The key here is that information is derived from the activities that ultimately provide focus to the monitoring component.
- The process does not depict the integration with the information and communication component of the COSO internal control framework. Effective reporting and communication, as well as correction and follow-up, are important components of an overall system of internal control. As with the risk assessment and control activities layers discussed previously, it is important to remember that "monitoring" is an integral part of the overall system.
- More control is not necessarily better control. At some point, the addition of controls begins to detract from the efficiency and profitability of a process without adding an equitable level of corresponding risk mitigation. Likewise, more monitoring is not necessarily better monitoring, which is why a focus on key controls allows an organization to focus its resources on the controls that matter the most.

As noted in chapter 2, the COSO internal control framework can be applied to multiple objectives (e.g., financial reporting, operations and compliance) and to multiple dimensions of an enterprise (department, business unit, etc.). Ultimately, there must be correlation between the controls that are being defined as key controls and the relevant monitoring activities. While this concept is fairly straightforward when applied to a business function or process, it becomes more complicated when determining how IT is considered because:

IT professionals need to be aware of these issues when considering their involvement. Communication, education and integration are essential elements of ensuring that these types of issues are properly considered by the enterprise.

- Many aspects of IT apply to multiple parts of an enterprise. For example, many application programs (e.g., an enterprise resource planning [ERP] system) are used across multiple departments and processes (e.g., accounting and inventory management). Similarly, certain IT processes (e.g., application development) might apply commonly to multiple application programs and, conversely, a given department that uses different application programs may have to deal with many discrete application development processes.
- Controls can exist for multiple purposes and operate at different requirement levels. For example, certain security controls that might be relevant to financial reporting (e.g., Sarbanes-Oxley) objectives might also be required for compliance with a business agreement (e.g., payment card industry [PCI]). While the same basic type of control is required, one control (in this case, PCI) might have a much more rigid control expectation than another because the nature of the risk and its impact on a specific business objective is different.
- When considering the potential for automated monitoring, tools that might not be justified when looking at a discrete process or part of a business might be justified if applied to multiple parts of an enterprise or processes, thereby increasing their value.

Step 1. Understand and Prioritize Risks to Organizational Objectives

The purpose of this guidance on monitoring is not to define how a risk assessment should be performed, but it is imperative that one be performed to implement an effective approach to monitoring. Risks can be prioritized only when considered against organizational objectives. This is complicated by the fact that not all organizational objectives are formally stated. This is of particular importance with respect to IT because there are several IT-related organizational objectives that are frequently "implied." For example, an enterprise may have specifically defined objectives for aspects of IT including:

- Complying with industry security standards (e.g., ISO/IEC 27002 or PCI DSS) or privacy regulations (e.g., US Health Insurance Portability and Accountability Act [HIPAA])
- Protecting proprietary trade information from theft
- Achieving 99.999 percent network availability
- Ability to restore 100 percent of mission critical systems and data within three days of a disaster

However, when looking at risks in a given business process that utilizes an IT application program, rarely will an enterprise formally define an objective relating to the "validity or integrity of transaction data." However, these are both likely to be considered "implied" objectives. Similarly, when stating broad objectives relating to new or upgraded application systems, there are usually implied objectives relating to "meeting user defined requirements" that are not always specifically stated.

IT professionals need to play a key role in ensuring that relevant stated and implied objectives are being considered when identifying and prioritizing risks.

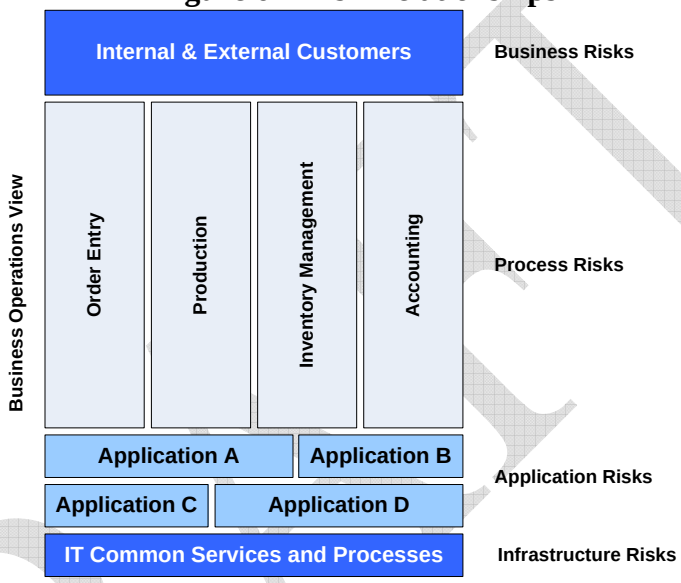
Appendix H provides information on the COBIT business information criteria that can be used as a framework for considering stated and implied objectives when focusing on business processes. These include:

- **Effectiveness**—Describes information that is relevant and pertinent to the monitoring process as well as delivered in a timely, correct, consistent and usable manner
- **Efficiency**—Concerns the provision of information through the optimal (most productive and economical) use of resources
- **Confidentiality**—Concerns the protection of sensitive information from unauthorized disclosure
- **Integrity**—Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations
- **Availability**—Relates to information being available when required by the monitoring process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance**—Deals with meeting the requirements of the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies

- **Reliability**—Relates to the provision of appropriate information for management to operate the enterprise and exercise its fiduciary and governance responsibilities

The identification of relevant IT risks within an enterprise should also consider the relationships among applications, databases and infrastructure that support the enterprise's business processes relevant to the defined objectives. This relationship is depicted in **figure 6**.

Figure 6—Risk Relationships



One of the core roles that IT professionals need to play in developing an effective monitoring plan is ensuring that meaningful risks are being identified.

Every business and IT process carries some degree of inherent risk, but the nature and level of risk vary between enterprises. Risk can be affected by a number of internal and external factors, such as the maturity of the enterprise; the complexity of operating models, business processes or IT; and the overall business and competitive climate. Enterprises should also consider the complexity of their application programs when prioritizing IT-related risks. Complex application programs are typically considered to be those that:

- Perform calculations that cannot be easily verified by users
- Are the actual source of the initiation of transaction or accounting-related events
- Handle such a volume of transactions that an independent review or analysis of processed results (to verify completeness and accuracy) is not feasible or meaningful

Although specific risks are unique to an enterprise, there are broad categories of risk that are commonly relevant to the determination and prioritization of specific IT-related risks, including:

- Application programs are used by those not authorized or trained to use them.
- Transaction data are inaccurate or invalid.
- Application programs do not work as intended or required.

- Data are stolen or added, altered or viewed improperly.
- Processing failures result in incomplete, inaccurate or lost data.
- Application programs are not available or do not perform acceptably.

Enterprises that have complex systems typically have a higher degree of risk in these categories than enterprises with less complex systems. For example, an enterprise that utilizes mostly packaged ERP software may perceive less risk in not having well-defined programming standards in place (since the enterprise does not have access to source code anyway) and place more risk upon not having effective change management processes and controls in place. It should also be noted that just because one aspect of an enterprise's IT environment is "complex" does not mean the entire environment is complex. In an enterprise with multiple IT environments, which is not uncommon among large enterprises, the nature and level of risk can vary between different IT environments.

To identify key controls to monitor, the IT professionals designing monitoring procedures must first understand (1) how the internal control system (as a whole) is designed to manage or mitigate identified meaningful risks, and (2) how that control system could have a failure not being detected in a timely manner.

Meaningful risks are those that, in a given time frame, might reasonably have a consequential effect on an organizational objective. The definition of risks initially should be at a fairly high level and be done in an integrated fashion (with non-IT personnel), especially when focused on business processes. At this point in the process, the only focus should be on identifying the relevant risks, not the controls. The process of defining meaningful risks and prioritizing them requires judgment and experience.

When identifying meaningful IT-related risks in a business process, it is sometimes helpful to allow the non-IT related risks to be identified and prioritized first to give context to the definition of IT-related risks. Using this technique will frequently provide more focus to the consideration of IT-related risks and also ensure that IT resources are not being devoted to areas that are not deemed to be significant risks. For example, if a business process has a complex application program that was purchased from and supported by a vendor, there is no reason to focus on application development risks.

Step 2. Identify Key Controls and Develop a Strategy Suitable for Monitoring

Monitoring should generally be focused on "key controls." Key controls are those that provide support for a reasonable conclusion about the effectiveness of the internal control system's ability to achieve the underlying objectives. By selecting "key controls" that address "meaningful risks," management can efficiently focus its efforts and resources on high-value controls.

The definition of what a key control is will vary from enterprise to enterprise and even between functional areas of a single enterprise. 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 them before they can become material to the

enterprise. Still other key controls may be defined by regulation or vendor agreements.

Key controls often have one or both of the following characteristics:

- Their failure could materially affect the ability to achieve an organizational objective but might not be detected in a timely manner by other controls.
- Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization's objectives.

As noted previously, identifying key controls starts with developing an understanding of how the internal control system as a whole works to mitigate meaningful risks. This understanding can be developed in a variety of ways:

- **Top down**—A top-down approach generally starts with a very high-level depiction of a defined area or process. Given the defined set of meaningful risks (as defined previously) places where risks are mitigated are defined starting from the highest level and then working backwards until all relevant controls have been identified. As needed, more detailed analysis is performed in areas where it is not clear either where risks might manifest themselves or how they are controlled.
- **Bottom up**—A bottom-up approach might start with a high-level depiction of an area or process but then work is performed to document the detailed processes and/or transaction flows in that area. From this information, specific places where risks can manifest themselves are identified along with the ways those specific risks are controlled.

There are times when either approach might make sense. In a top-down approach, most controls identified will likely be key controls because of the way they were identified (i.e., in a top-down fashion). Typically, in a bottom-up approach it is necessary to determine from the numerous controls identified in the process which are key controls. This is an analytical process that should focus on the way the meaningful risks are best controlled.

Regardless of which approach is used, the identification of key controls can be facilitated by considering factors that increase the potential that the internal control system will fail to manage properly or mitigate a given risk. The COSO 2009 guidance identified several factors (which are equally applicable to both IT and non-IT related controls) including:

- **Complexity**—Controls that require specialized skill or training typically are more susceptible to failure than simple controls.
- **Judgment**—Controls that require a high degree of judgment, such as controls over the determination of valuation allowances, are highly dependent on the experience and training of those responsible for the judgments and are often associated with meaningful risks.
- **Manual vs. automated**—Manual controls are more susceptible to human error than automated controls and, as a result, are often subjected to different levels of

monitoring than automated controls (e.g., they may be evaluated more frequently or employ larger sample sizes when sampling is performed). However, when automated controls fail, they tend to fail repeatedly in the same circumstances and, therefore, need to be subjected to an appropriate level of monitoring when they address meaningful risks.

- **Known control failures**—Previous control failures are a clear indicator of the need to increase monitoring activities until corrective actions have effectively addressed the cause of the control failure.
- **Competence/experience of personnel**—Inadequate competence or experience in performing a given control increases the likelihood of control failure.
- **Potential for management override**—Controls that might be overridden by management for purposes that are contrary to organizational objectives may warrant specific monitoring attention.
- **Likelihood of control failure detection**—If other controls within the internal control system can reasonably be expected to detect a given control failure before it becomes material, that fact may decrease the need to identify the given control as key. Conversely, if it is reasonable to believe that a control's failure could be material and yet not be detected and corrected on a timely basis, the need increases to identify the control as key.

The specific types and placement of key IT-related controls to address defined meaningful risks will vary considerably based on:

- The size and sophistication of an enterprise
- The sophistication and complexity of its application programs
- The scale of its overall technology "footprint" (e.g., the types, numbers and locations of IT resources deployed)
- Its organizational philosophy

Some enterprises have very centralized IT processes and decision making; others follow a more decentralized approach. These differences can result in a different assessment of the relative importance of specific IT controls.

For example, in an enterprise with 15 business units operating a centralized IT environment with a single integrated ERP system, the importance of program change controls is much greater than in that same size company operating a decentralized environment with discrete ERP applications. This is because, in the latter example, an individual unauthorized change would affect only one of the 15 business units.

Key IT-related controls are typically defined at two levels:

- **Controls related to application processes** (often referred to as application controls)—Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. There are numerous types of application controls, ranging from a combination of manual/programmed controls (e.g., user review of the computer-generated exception report) to entirely computer programmed controls (e.g., only valid

numeric data are entered into an application). These controls are implemented through a combination of access rights and authorities, application program design, programming logic, and application configuration.

- **Controls over IT common services and processes** (often referred to as IT general controls or ITGC)—Controls, other than application controls, which are related to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to most applications. These controls are typically implemented through a combination of policies and procedures, system software, and segregation of duties considerations.

Examples of Key Application Controls

It is difficult to generalize about what types of application controls are going to be considered key. Application controls always are designed to support a given business process and there are immeasurable combinations of business processes (and related application programs) used in different ways across enterprises and industries. The following four types of control situations provide examples of situations where controls might be considered key controls:

- When access to key aspects of an application or segregation of duties between functions of an application control are considered important controls to mitigate a risk, then application security will generally be considered a key control.
- In transaction processing, to the extent that the determination of invalid vs. valid transactions is important and performed by an application program, this control will be considered key.
- Where workflow or similar rules require a system-based supervisory approval or the override of an otherwise significant control, the programming logic and parameters that enable this functionality will be typically considered key.
- To the extent that there are system-based processes that ensure the completeness of transaction processing or significant system interfaces, this control will likely be considered a key control.

Examples of Key IT General Controls

Virtually any of the controls and control objectives defined in COBIT might ultimately be considered a key control depending on organizational objectives and meaningful risks. Examples of key IT controls that may be considered for monitoring are:

- **Limited access to source code**—The ability to make programming changes (including application configuration changes) is limited to specific personnel who are both trained in programming tools and authorized to make programming changes.
- **Systems security**—Access to IT resources is restricted to valid users and the network is protected from intrusions.
- **Data and database security**—The ability to add or alter data (both master file and transaction data) is limited to individuals who are using approved and

authorized application programs or database administrator (DBA) tools (because these programs typically provide an audit trail of activity that can ultimately be reviewed).

- **Limited access to production**—Only personnel with a justified business need are granted the ability to modify the production environment.
- **Program testing—**Programs, including controls within applications, are tested to ensure that they work as intended prior to being moved into a production environment.
- **Program change control** (including application configuration)**—**Changes are authorized to ensure that only approved changes are applied to production programs. It is important to note that, as discussed previously, in most modern application programs, there are certain key controls that are "configurable" in that they are based on parameters stored in database tables and used by the application to impact aspects of its operating logic.
- **Performance management—**The use of technology resources is planned and managed to ensure that systems are available and perform at satisfactory levels.
- **IT portfolio management**—A prioritization and approval process exists over the acquisition and deployment of IT resources.
- **Job scheduling—**IT "jobs" are approved, scheduled and managed to enable complete and accurate processing of data and information.
- **Operational data redundancy—**Processes are in place to ensure that the enterprise does not lose data due to outages or disasters. There are typically numerous methods to accomplish this, including data mirroring and tape or disk backups.

One of the key activities that IT professionals need to undertake is ensuring that controls are operating at the right level to manage a defined set of risks.

A sample of key IT controls, information used for monitoring and a description of the related monitoring process are included in appendix E.

These are broad categories of controls. COBIT and other resources, such as ITIL, should be considered when determining the specific controls in these broad areas. It should be noted that the areas discussed previously deal only with the essence of what the control is, not the level to which it must operate to manage a given risk effectively. There is a significant variance in the degree to which controls in these areas need to be implemented based on the risks. For example:

- Access to a given transaction or resource should consider the business requirements and all of the other controls in place. In certain situations (such as the ability to make a wire transfer) the access restrictions might be considered much greater than in other situations (such as the ability to enter a sales order) where there may be additional controls that would prevent a significant business impact.
- Segregation of duties within IT and between IT and other parts of a business should be based on a given scenario. In cases involving complex systems, it is more important to segregate duties between application developers and database administrators than it might be in enterprises with relatively simple systems. In these latter cases, where users have the ability to review or reconcile a business activity, the segregation of duties requirements might be limited to ensuring that

the business users have no access to application development or databases.

- Data center security in an enterprise may be adequately addressed by physically securing IT resources in a dedicated, locked room; while another enterprise may need to implement sophisticated authorization requirements, movement sensors and cameras to meet data center security needs, based on their unique risks.

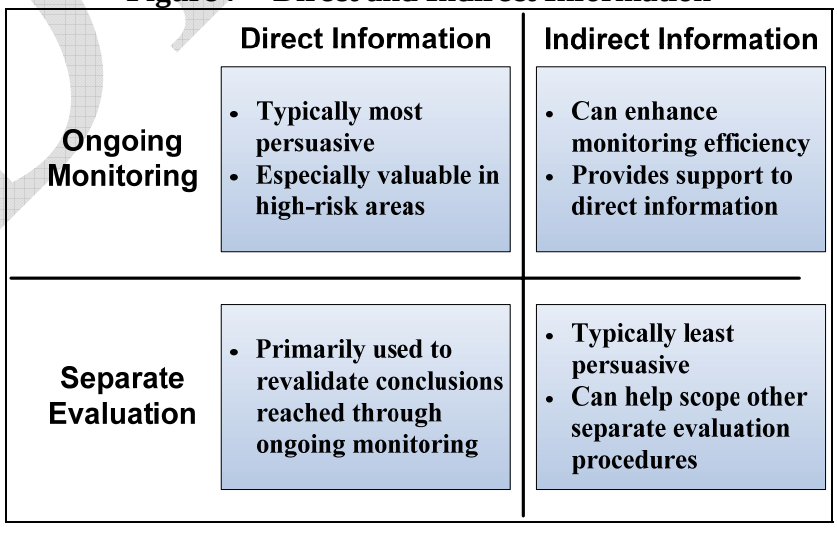
In these examples, the decisions as to the level that a control must be implemented can be made only after understanding the role that access restrictions play in managing a defined set of risks.

Step 3. Identify Information That Will Persuasively Indicate Whether the Internal Control System is Operating Effectively

Once key controls have been identified, consideration should be given to the various options that exist to monitor those controls. This exercise requires considerable thought as there are various ways in which controls operate that impact how they can be monitored. The ultimate purpose of monitoring is for an evaluator to gather enough *persuasive information* to conclude that a control is operating at a sufficient level to mitigate a meaningful risk.

As explained more completely in chapter 2, *persuasive information* is both *suitable* and *sufficient* for the circumstances and provides the evaluator reasonable support for a conclusion regarding the continued effectiveness of the internal control relating to a defined set of organizational objectives. *Suitability* considers the relevance, reliability and timeliness of information about the operation of a control and *sufficiency* is a measure of the quantity (i.e., amount) of information. In addition, the monitoring of key controls can be achieved by using a combination of *direct* and *indirect* information (see chapter 2 for an explanation of the difference between direct and indirect information). **Figure 7** provides a quick reference on the relative persuasiveness and use of direct vs. indirect information.

Figure 7—Direct and Indirect Information



The key point for IT professionals is that this exercise requires judgment, communication and thoughtful consideration in defining what key controls exist. Most important, in many cases key IT-related controls need to be considered on an integrated basis with non-IT controls to ensure that the enterprise both understands and is focused on the right things.

An additional factor, which is inherently part of the decision as to whether and how direct and indirect information are used, is the intended role of the monitoring activity. For example, publicly traded organizations in the US might be using monitoring as a key element of their quarterly 302 and annual 404 Sarbanes-Oxley compliance requirements relating to financial reporting. In these cases, because the inherent legal and regulatory risk is higher, an enterprise will typically place more emphasis on direct information than it might for operating controls that are not part of an external reporting requirement and not subject to quarterly or annual public reporting.

Whether information is direct or indirect is sometimes a difficult determination to make, particularly considering the fact that some activities are "dual purpose" in that they operate both as a control and a monitoring activity. Examples of these are discussed in the following text. Although indirect information cannot, by itself, provide positive assurance that a control is operating effectively; it can be an indicator of when a control is failing. To the extent that this information is then used to investigate a problem and take corrective action before the problem becomes significant, this activity is probably "dual purpose" in that the "identify and correct" activities are the essence of how a detective control operates.

Another factor that needs to be considered is the volume of indirect information that is being examined. This is an especially significant issue when considering the use of automated tools. As noted in paragraph 101 of Volume II of the COSO 2009 guidance:

> *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). 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.*

In this example, these tools are potentially looking at indirect information because an evaluator must *infer* the operation of a control when looking at the information. However, if an organization examines a sufficient set of transactions in this fashion, it is likely that this is a "key control" that is being implemented through "ongoing monitoring," which would seemingly reduce the need for separate evaluations of an application or other controls in this defined area.

There are four main tasks that should be performed in this step to determine:
1. The nature of the key control that needs to be monitored
2. Whether a specific control is already being monitored
3. The information sources available for monitoring
4. The feasibility of using automated tools

As these tasks are performed, there are considerations that need to be made throughout all of the activities, including:
- How significant or meaningful is the risk that is being addressed?
- How directly does the control address a defined risk when considered against other potential controls?
- What is the nature of the control? Is it manual or automated, detective or preventive?
- Does the effectiveness of a control potentially depend on other controls (e.g., aspects of security or application development)?

Task 1. Determine the nature of the key control that needs to be monitored.

A critical first step in this process is clearly defining the elements that make up a given key control. Although many key controls might have only a single element, others may have multiple elements. For example:
- A stated control that "all requests for a network ID must be signed by a department head" is straightforward and made up of a single element (i.e., the signature of a department head).
- A stated control that "system settings require a user to change passwords every 60 days" likely has multiple elements since it is based on both the fact that a system parameter is set at "60" and that it is not changed.
- A stated control that "all programming changes must be subjected to a comprehensive test plan based on the significance of the change" has multiple elements to it because the competence of the people defining test plans and evaluation of the significance of a change are inherent elements of the control that needs to be monitored.
- Access controls always have at least two elements. The first element is the programming logic built into the application or infrastructure resource that allows or disallows activity based on certain constraints and the definitions of access rights. The second element is the provisioning of those constraints and/or access rights to individual users of the resources.
- An "application control" (e.g., a tolerance or limit placed on a field within a transaction record) is typically based on programming logic that is part of the functionality of the program. It may also be based on configurable parameters that users provide and that the programming logic uses as the program operates.
- Certain application controls are "built in" to the functionality of an application. For example, in the accounts payable aspects of an ERP system it is common that an invoice can be processed only for:
  – A previously established vendor

  - Purchasing an existing and established product
  - A previously approved price on a purchase order (PO)
  - Where there is a record that the product was physically received

  These four controls are part of the inherent logic of the application, but each is totally dependent upon the process whereby the master files that support vendors, products and POs are maintained. As such, it is important that the monitoring of controls is focused on those activities that enable control in the application.

The purpose of this activity is to ensure that all elements of a key control are ultimately being considered when determining monitoring options. For example, a network scanning tool might easily be able to determine if the password setting in the example in the second bullet in the previous list is something other than 60, but that same tool might not be able to tell if, or how frequently, that setting had been changed over a given period. Thus, when defining a monitoring plan, it would be important to consider both aspects of the control.

Task 2. Determine whether a specific control is already being monitored.

Once the nature of a key control has been identified, the next step is to determine if the control is already being monitored through a routine business process or other control activity. It is not uncommon for a control to be monitored by a subsequent process. For example, consider the following example based on a program change control process:

- A department head must sign off on the design specifications for a new system and on the fact that the final version of the change meets the defined requirements.
- All program changes are reviewed by a Change Review Board made up of key IT leaders. The Change Review Board will not discuss any changes that have not had both sets of approvals evidenced by the signature of a department head and the report from a weekly meeting where the department head participates in the discussion of the purpose and impact of the change.

In this case, the Change Review Board is, potentially, monitoring aspects of the control relating to the approval by the department head. This is only potentially considered a monitoring activity because there are several pervasive issues with respect to identifying whether such monitoring activities already exist, including:

- Is the evaluator of the information competent, objective and aware that he/she is performing monitoring?
- When exceptions are identified, are they evaluated and communicated as control deficiencies or failures in such a manner that would allow the impact of the deficiency on the overall system of internal control to be evaluated?

The following activities are examples of IT processes that, if implemented properly,

might provide management information about the operation of their controls. Certain of these processes provide "direct" information about control effectiveness meaning that there is a specific relationship between the activity that is being performed and a specifically identified control. Other processes provide only "indirect" information in that they provide information at a much higher level, or perhaps on a more composite basis, than a specific control. Examples of IT processes providing control information are:

- **Access recertification, direct—**A security access recertification is a process through which the existing access rights to a given IT resource (e.g., an application program or a component of infrastructure) at a point in time are provided to the person responsible for that resource. The responsible person then compares the list to what he/she expects and identifies potential exceptions. The potential exceptions are then investigated and addressed, as required. Because this process occurs outside of the normal process for adding and changing user access rights, done correctly it serves as a method of monitoring whether the security administration process (whereby user access rights are added, changed or removed) works effectively.
- **Security log monitoring, indirect—**A common control in any IT environment is the process of "signing on" to an IT resource using some combination of user ID, authentication device and password. Many organizations log this activity to provide an audit trail of who is using IT resources. Because the logging process also records failures, where either the user ID did not exist or the password is incorrect for a valid user ID, an analysis of access failures is a fairly common procedure that provides information to security management personnel about whether there is any unusual activity occurring. This, in turn, provides indirect information about certain aspects of the security environment. This activity provides only indirect information to management about the effectiveness of the internal controls since, by definition, the information that is being monitored represents an analysis of failures to gain access to information resources.
- **Portfolio management and/or steering committees, indirect—**IT portfolio management can mean different things to different enterprises and it can be implemented in many different ways and at different levels of detail. At its base level, however, IT portfolio management provides a means for understanding and properly prioritizing requirements and then allocating IT resources (including costs) to those requirements. To the extent that IT activities are then periodically compared to the defined requirements, a portfolio management process can provide an indirect means by which management assures itself that IT development efforts and IT resources are being devoted to those activities that have been approved by management.
- **Independent quality assurance or peer review over program development, direct**—In many larger IT environments, there may be an independent quality assurance function (or a peer review process) that reviews all proposed program changes prior to their movement into the production environment. In this process, the quality assurance team looks for evidence of testing and required approvals. In some cases, this function may also independently verify key aspects of the underlying process. To the extent this process works on

application systems that are relevant to internal controls over financial reporting, this activity might be considered an effective monitoring of the underlying controls relating to testing and user signoff.

- **Change review board, direct and indirect—**In enterprises where changes to the IT environment are both frequent and potentially disruptive, some organizations have implemented a "change review board" to provide oversight to the change process. A change review board is typically made up of cross-functional IT (and possibly business unit) managers who collectively review and approve all changes after satisfying themselves that all requirements for the change have been met (approvals, testing, communication, etc.) prior to the change being approved for movement or production. Similar to the activities discussed previously under independent quality assurance, if this function works effectively, it may provide evidence that management is monitoring the controls relating to user signoff and testing. Whether this activity provides direct or indirect information about the effectiveness of controls relates specifically to the level of depth and oversight that the change review process provides.
- **Post-implementation reviews of program changes, indirect—**Similar to the independent quality assurance processes discussed previously, to the extent that an enterprise performs a post-implementation review of major program changes, the review process can provide indirect information about the effectiveness of its internal controls over the development process. The distinction here is that this activity is typically performed after a program has been placed into production and is being used in the enterprise. The most effective post-implementation review processes include both an evaluation of the functionality and usefulness of the program as well as the effectiveness of the internal controls that are built into the application programs and the business processes.
- **Problem management, indirect—**Many IT organizations have sophisticated "problem management" processes in place. Problem management is different from, but related to, incident management. The purpose of incident management is to return IT applications and services to a normal level as quickly as possible, with the smallest possible business impact. The principal purpose of problem management is to find and resolve the root cause of a problem, thereby reducing future incidents. An effective problem management function can provide management indirect information about the effectiveness of several different IT processes that may ultimately be determined to be the source of incidents.
- **Performance management, indirect**—Many IT organizations utilize a host of metrics to measure and analyze IT performance from a technical perspective. The vast majority of these metrics are operational in nature in that they measure important business requirements, such as system availability or processing performance. Some measures, particularly those relating to changes, may also provide indirect information about the effectiveness of internal control processes. For example, the following types of measures might provide indirect information to management about the effectiveness of the application development and change control processes:
  - Unplanned (e.g., emergency) development activity as a percentage of total development activity

  - Number of changes made per week compared to those authorized
  - Number of "first time" successful changes compared to the total changes made
  - Number of emergency changes
  - Number of service-affecting outages caused by changes
- **Recovery testing, direct—**IT management may choose to do different levels of testing of the capability to recover from different forms of disruptions or disasters. To the extent that this testing involves the reestablishment of IT systems that are relevant to financial reporting by using either backup tapes or redundant/mirrored systems, the tests themselves provide management direct evidence that the redundancy or backup controls work effectively.

It is also important to recognize that the overall size of an IT department has an impact on the types of monitoring activities that might be effective. Smaller IT departments that rely more on direct supervision and review (as opposed to formally structured and measured processes) may have different methods for accomplishing the monitoring activities described previously.

Task 3. Determine the information sources available for monitoring.

Determining direct information sources is fairly straightforward in that they provide direct information that a control is operating. Focusing on the elements of a control as defined previously will provide focus to this effort and ensure that all sources are being considered. A monitoring approach utilizing direct information would typically require the use of reperformance, examination or observation. In this process, however, it is important to recognize that the term "information" could easily be replaced with the audit term "evidence" and that the "evidence" of many controls, especially those requiring judgment and expertise, is not frequently captured in information systems. Accordingly, the direct information that supports many controls will need to be derived through observation by the evaluator.

Indirect information sources are not always as clear as direct information sources. Since the intent of indirect information is to point out control failures, thereby allowing an evaluator to gain an inference about whether a control is operating (when there is no indication that controls have failed), there needs to be a strong correlation between the key control (or elements of control) and the information. The discussion in the immediately prior section provides a few examples. However, this is not an exhaustive list. Enterprises are all different so there will ultimately be a myriad of potential indirect information sources. Performance indicators found in the COBIT framework can provide an excellent source for determining potential indirect monitoring measures.

In this determination, it is important to recognize that if a key control has a history of being ineffective and/or is relatively new, direct information about the control should be the focus until the control reaches a sufficient level of maturity and reliability.

The following two examples highlight how the combination of both direct and indirect information sources might be used.

Example 1

An ERP system typically requires that sales can be made only for products that have been previously defined in the ERP system. In addition, the price that a customer pays and the credit limit of the customer are defined in the ERP system through business processes that exist within the enterprise. In such a case, management typically needs some form of direct information that the controls over adding customers, inventory items, prices and credit limits work as intended. In addition, management typically needs some form of direct information that it has controls over the periodic verification of physical inventory levels. However, management may be able to utilize indirect information that comes from its operations to satisfy itself that other controls are working. For example:

- Assuming that the enterprise periodically compares finished goods inventory levels to the perpetual inventories in its ERP system, the lack of any significant differences between perpetual levels and actual levels provides indirect information that its billing controls are operating. Note, however, that this does not provide any information about the propriety of cut off, for which management needs to have direct information.
- Reports that provide information about any unusual deviations and individual product margins (whereby the price of an item sold is compared to its standard cost) provide indirect information that controls over billing and pricing are operating.
- The monitoring of the cause of credit memos can also provide information about billing controls, especially in situations where it is possible to identify whether credit memos were issued for shipping or pricing disputes. To make a proper inference about these controls, management would also have to satisfy itself that there is no adverse deterioration in aging of its receivables for its customers.
- Reports that show orders that were rejected for credit limitations provide indirect information that credit checking aspects of the system are working as intended. To the extent that an "override" can be used to allow a credit limit exception, these reports can also be used by management to satisfy itself that the process of approving these overrides is operating.

Example 2

In certain business situations (e.g., the automotive and retailing industries) it is not uncommon for customers to pay for items received based upon the customers internal recording of what was received and the price that the customer agreed to pay. In such situations, an enterprise's internal billing system is used principally to allow it to record revenue and inventory relief—invoices are frequently not even sent to customers. In such situations, management's review of accounts receivable aging and the issuance of credit memos can provide valuable indirect information about whether internal controls over billing and pricing are working as intended. In

such situations, the enterprise's internal billing system becomes an element of the internal control, since customers are not paying based on an actual invoice being sent. Note that in these situations, management would still require direct information over the controls relating to achieving a proper cut-off at the end of a period.

Enterprises that are considering using automated tools should focus on what they do and how they work, not what they are called.

Task 4. Determine the feasibility of using automated tools.

Although chapter 4 is devoted to the discussion of using automated tools, the topic is covered here because it is an integral component to identifying and using persuasive information to indicate whether the internal control system is operating effectively.

Automated monitoring tools may add value to the monitoring process in situations where the information that supports a conclusion that a control is in place and operating resides directly or indirectly in electronically stored data. Monitoring tools can focus on many, but not all, dimensions of internal control. Some tools focus on a very narrow set of control issues, others cover a broader range. Software vendors use varying names to describe what their tools provide. Software tools that do the same basic thing can be called by different names, and conversely, tools with the same basic names can do entirely different things. Further, some tools are designed to focus on monitoring or auditing internal controls, others are integrated into IT operating processes but provide essential information that is relevant to monitoring.

Before discussing the specific types of tools that might be used, it is important to note that:

- Many tools are likely to be considered "multipurpose" in that they are designed to provide a form of operational process or control. However, depending how they are used, these tools can also provide direct or indirect information to management that controls are in place and operating.
- Just because a tool is in place, it does not mean that monitoring is actually being performed. To be considered here as effective for monitoring of controls, there needs to be a focus on communicating results/issues from these tools to those responsible for evaluating internal controls (e.g., evaluators).

Examples of various types of software tools that can be used to perform different types of control monitoring are summarized in the following text. These tools are organized into groups based on the focus of the tool as it relates to monitoring internal control, specifically:

1. Transaction data
2. Conditions
3. Changes
4. Processing integrity
5. Error management

Although automated monitoring tools can be highly effective in a number of situations, they are not without their limitations. Some of these limitations are that automated monitoring tools generally cannot:

- Determine the propriety of the accounting treatment afforded individual transactions, since this must be determined based on the underlying substance of the transaction itself
- Address whether an individual transaction was accurately entered into the system; they can deal only with whether the transactions met internal standards for acceptable transactions (i.e., it was valid)
- Determine whether all relevant initial transactions were entered into systems in the proper period, since this is typically dependent on human activity

Chapter 3 discusses the use of automated tools in more detail and presents considerations when selecting and implementing such tools.

Example 1. Transaction Data

Tools for evaluating transaction data compare individual transactions that have been processed against a set of control rules to highlight exceptions. The intention of these tools is to identify instances in which the controls over a process or system are not working as intended. This category of tools can provide monitoring information such as:

- Highlighting exceptions and/or anomalies
- Analyzing unusual trends in activities, values and volumes
- Comparing balances or details between two systems or between distinct parts of a process

Tools in this category can take the form of *ad hoc* programs that are run periodically against the defined population (either a sample of the data population or the entire population) or programs that are implemented into a processing environment to continuously monitor a specific set of transactions.

Because of their ability to be used in a variety of situations and to correlate data and information from multiple sources, there are an immeasurable number of situations where tools might be used to:

- Highlight significant manual or unusual automated journal entries so that financial management can ensure that such entries were proper and approved.
- Search for unusual or duplicate payments so that management can ensure that controls over disbursements are working effectively.
- Analyze unusual activity as part of management's fraud-prevention activities.
- Determine the frequency of supervisory overrides.
- Validate that all transactions fall within a specific control range.

These are just brief examples, as the possibilities are endless. Generally tools used in this fashion tend to deal with controls designed to focus on the integrity of transaction processing. Because they deal with processed data, they can also be used to confirm the controls relating to the completeness of processing but only

from an internal perspective (i.e., they cannot evaluate whether all transactions were entered into a system, but they can evaluate the completeness of transactions being moved from one system to another).

The previous examples also highlight the sometimes subtle difference between a control activity and a monitoring activity. As discussed in the introduction to this section, many of the situations where tools of the fashion described are actually performing a control activity. In the journal entry example, an independent review of journal entries to determine if they are approved describes a detective control. But, if in this activity management finds no situations where journal entries are not being approved, it provides indirect information that the control over approving journal entries is working. Conversely, if it finds exceptions, management can take steps to determine why the control over approving journal entries is not working and take steps to correct it.

Example 2. Conditions

This category of automated tools monitors the settings and rules that govern IT processing. Many "controls" that are built into systems are controlled through the configuration of a specific set of parameters within both IT infrastructure resources and application systems. For example:

- Certain security controls and policies are enabled through parameter settings in the base operating system or within the configuration of an application system (e.g., controls such as the length and complexity of passwords and the frequency with which they need to be changed are enabled by security parameters).
- Certain controls within application systems depend on the base configuration of the application. These configuration options can affect transaction processing (billings, payments, etc.) and/or the integrity of the application environment (security parameters, change control, etc.). For example, whether an ERP system uses LIFO or FIFO when accounting for inventory activity is dependent upon the parameters that define the application configuration. Similarly, tolerance levels for processes that match activities typically are based on configuration information.
- Within application systems, the ability to segregate incompatible duties is enabled by application security rules that are based on an enterprise's definition of roles and the access associated with those roles. For example, incompatible duties within or between application systems are identified by comparing existing user access rights to a baseline set of incompatible rights, either within a single application or across multiple applications.

Software tools in this category typically examine specific settings or parameters that control how an application or infrastructure resource is configured, and then compare the configuration information to either baseline information, a prior analysis, or both to determine if they are consistent with the enterprise's expectations. Software tools in this category increase the speed and effectiveness of the monitoring process while simultaneously allowing it to be performed on a more frequent, or even continuous, basis. These tools can be of particular value in

situations in which:

- A large number of conditions need to be evaluated in a relevant IT resource (e.g., numerous parameter settings affecting internal control in an integrated ERP system, or multiple different "instances" or versions of the same ERP package that support different business units).
- Relatively few parameters need to be evaluated across a large population of resources (e.g., analyzing security parameters across relevant servers in a global network).
- The conditions that need to be evaluated are complex and/or too time-consuming to perform manually (e.g., when there is a large number of users of a single application or multiple applications to be evaluated for appropriate segregation of responsibilities as defined by application access rights).

These tools may operate periodically (frequently described as "scanning-based") or can be embedded in the process as either software or hardware (frequently described as "agent-based"). Determining the best approach for an enterprise should be driven by the importance of the control and the related risk that control is designed to mitigate. There are trade-offs with respect to these solutions that need to be considered carefully by management in the process of determining whether tools of this nature will work in their environment.

These types of tools typically deal with integrity controls and there are dimensions of these controls that support access and authorization-related controls as well. This is particularly true for tools that analyze security-related parameters, as these parameters typically are relevant to ensuring that only those authorized to utilize resources can gain access.

Example 3. Changes

Change-monitoring tools are an extension of the tools that focus on "conditions," as just discussed. The basic difference is that these tools usually operate on a continuous basis (i.e., they are "agent-based") and are specifically designed to identify and report changes to critical resources, data or information, thereby making it possible to verify that changes are appropriate and authorized.

Change within IT resources is pervasive, continuous and unavoidable. When controlling change is considered a key control, enterprises typically have some form of "change control" that includes both a preventive control that limits the ability to make changes to specific personnel and a detective control whereby all changes are recorded, reviewed and, potentially, approved by someone independent of those making changes. For example:

- Changes that have been made to database structures can be logged by the database environment itself and then subsequently reviewed by management.
- Certain ERP environments provide their own control mechanism for making programming changes or changes to the ERP configuration. To the extent that this exists, the reports of these changes can be used as both a detective control and a means by which management monitors controls.

Although this approach to controlling change works effectively, it is dependent upon the ability of the resource being changed to provide an effective means to record changes and thereby ensure that any changes can be reviewed and approved. However:

- Not all IT resources provide the capability for recording changes.
- In large IT environments, the number of individual resource components that would need to be analyzed on a detective basis can be overwhelming.
- Using native logging capabilities of some resources may affect system performance unacceptably.
- In certain high-risk areas, management may not wish to use the native features of certain resources because of the simplicity of turning off these features.

When these conditions are present, tools in this category can become mechanisms for both control and monitoring. As such, they can identify changes that have been made to infrastructure resources, databases, application programs, and security rights and permissions. These tools can provide visibility for all changes so that ultimately they can be validated independently, which is, in essence, monitoring that the underlying change control process is working. These tools also can provide alerts when certain types of mission-critical changes are being made so that there is transparency throughout the enterprise and necessary actions can be taken on a timely basis. Lastly, they can provide a verifiable audit history for direct information of control functionality over time.

As with those tools that focus on conditions, these tools largely focus on integrity and authorization-related controls.

Example 4. Processing Integrity

Automated tools to evaluate process integrity are designed to verify and monitor the completeness and accuracy of the various situations that may occur in the overall IT process. Typically they focus on balancing and controlling data as it progresses through processes and systems. Tools in this category can perform activities such as:

- Reconciling financial totals and/or transaction/record counts from one file or database to another file or database, within the same or between different application or operating systems
- Ensuring data-file, record, and field accuracy as data move across systems and processes
- Monitoring information from source systems and/or data warehouses to the general ledger

Because these systems operate independently of transaction processing, they can also be designed to maintain an audit trail of key information for monitoring or trending studies. Within an enterprise, these tools are typically considered a control mechanism. However, depending on how management uses them, these tools could also be considered mechanisms for monitoring controls as they relate to information processing.

Example 5. Error Management
Error-management tools are designed to detect transactions that do not meet defined criteria so that they can be corrected and reprocessed. For example:

- An automotive parts supplier may receive a technically valid electronic data interface message describing an authorized shipping schedule. However, the message may have an invalid order identification.
- A telecommunications provider may receive message information from its telephone switching systems on customers whose information has not made it through the process of being added to the billing system.

The fact that invalid transactions are rejected is frequently considered an "application control." However, these systems frequently capture the transactions in an area where they can later be reprocessed after correcting the cause of the error. Management's monitoring of the volume and resolution of activity in these systems or accounts provides both direct and indirect information that the control is working effectively.

It is important to note that these capabilities typically are part of an existing information system rather than an add-on vendor solution.

Considerations for implementing automated tools are discussed in chapter 4, while an overview of common tools that may be used for automating the monitoring process can be found in appendix D.

These attributes should be considered by IT professionals in defining monitoring processes for IT-related controls.

Step 4. Develop and Implement Cost-effective Procedures to Evaluate that Persuasive Information

In this step, an enterprise first designs and then implements the combination of ongoing monitoring procedures and/or separate evaluations needed to gather and analyze persuasive information supporting conclusions about the effectiveness of internal control.

While the following section discusses the design and implementation of the monitoring process *per se*, chapter 4 focuses on the potential use of automated tools as part of the overall process.

Principle 19 of COSO's 2006 publication *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* provides several attributes of effective monitoring that can be applied broadly. Specifically, those attributes are:

- **Integrates with operations**—Ongoing monitoring is built into the enterprise's normal operating activities.
- **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 activities supporting the enterprise's objectives.

- **Considers feedback**—Management receives feedback on the effectiveness of internal control.
- **Adjusts scope and frequency**—Management varies the scope and frequency of separate evaluations, depending on the significance of risks being controlled, the importance of the controls in mitigating those risks, and the effectiveness of ongoing monitoring.

This step involves four broad tasks:

1. Determine the frequency and method for monitoring and define evaluators.
2. Develop monitoring procedures and determine changes needed to implement ongoing monitoring.
3. Select and implement automated monitoring tools.
4. Clarify reporting requirements and expectations.

Task 1. Determine the frequency and method for monitoring and define evaluators.

Ultimately, this is a unique judgment of the management of an enterprise after factoring in its objectives, its risks, its controls and the persuasiveness of information that is available about its controls. As noted in step 3, certain controls may already be monitored as part of an existing process. In these situations, activities may be limited to ensuring that the frequency of monitoring is sufficient for management's purpose. For other controls, this decision will need to consider several factors including:

- **What is the nature of the control?—**Answering this question should focus on the specific elements of the control, as discussed previously. In general, automated controls require less frequent monitoring of their automated aspects because once the control is verified to be working properly, automated aspects are unlikely to change unless change management controls within the system cannot be relied upon.
- **How will monitoring be used?—**A properly designed and executed monitoring program helps support both internal needs to ensure that objectives are being achieved as well as external assertions,[3] because it provides persuasive information that internal control operated effectively at a point in time or during a particular period. This duality of purpose ultimately should play a role in decisions made as to the frequency and method of evaluation as well as who should be the evaluator.
- **Who should best evaluate a given control?—**Answering this question provides needed input to the decision about how monitoring should best be performed. There are several criteria that must be considered relating to the competence and objectivity of an "evaluator" of an internal control that might have an impact on the ultimate decision being made in this activity. For example, if a decision is made that the CIO should evaluate a control, it is most

[3] External assertions are statements (usually in writing) to external parties regarding the effectiveness of internal control. They may be required by regulation or contractual agreement. They may also be voluntary.

likely that a decision will also be made that his/her monitoring would be part of an ongoing management process, not a separate evaluation.

- **What is the mix of direct and indirect information?—**When monitoring procedures can be utilized with highly persuasive information (i.e., direct information), monitoring can be performed on whatever schedule is deemed sufficient by management. If they use less persuasive information (i.e., indirect information), additional separate evaluations may be required more frequently.
- **Can we make the evaluation an ongoing process?—**To the extent that controls can be monitored through an ongoing process, it is more likely that control issues will be highlighted on a timely basis. However, not all monitoring activities lend themselves to being easily implemented as part of an ongoing process. This decision ultimately needs to be made by management for each unique situation.

Task 2. Develop monitoring procedures and determine changes needed to implement ongoing monitoring.

The specifics for each monitoring procedure need to be developed for both ongoing and separate evaluations. This activity focuses largely on the development of activities and reporting responsibilities and then training and change management activities for those impacted.

Task 3. Select and implement automated monitoring tools.

The selection and implementation of monitoring tools should follow the same basic technology acquisition and implementation processes that an enterprise uses for any of its business systems. In determining whether, and how, to use a given tool, there are several factors that should be considered, including:

- **Cost/benefit (return on investment [ROI]***)*—To the extent that a tool needs to be newly licensed, an enterprise must understand the total cost of ownership when it chooses to purchase and use a monitoring tool. Licensing costs for software are only a very minor part of the total cost of ownership for tools. Each of the factors noted previously must be considered in terms of the benefit of automating the monitoring process compared to alternatives.
- **Sustainability**—Technology applications and infrastructure change frequently. Accordingly, it is important that any form of monitoring software be able to change with the same rate of speed to be effective. If monitoring tools do not change at the same pace as the underlying applications, there is a risk that there will be no monitoring of new or changed controls in the application. Although more of an efficiency issue, they may also identify control deficiencies that are not real, resulting in a waste of resources to investigate and resolve discrepancies.
- **Scalability**—To be of value, monitoring tools have to be able to keep up with the growth of an enterprise. Accordingly, it is important to consider the ability of a monitoring tool to meet anticipated growth in process, complexity or transaction volumes.

- **Customizability**—Many software products come with "rules" that have been defined by the vendor, based on their mapping to control frameworks available in the marketplace. These rules frequently do not meet management's criteria. Effective software must be able to focus on "things that matter" so any tool must be able to be customized to the specific needs of an enterprise. The ability to customize should, to a large extent, be built into the software so users can adapt the software as opposed to programmers—the cost of custom programmer changes to parameters or rule sets can be prohibitive and impact scalability.
- **Ownership**—Someone in the enterprise must "own" the tool and be able to identify effectively organizational changes and opportunities that would necessitate changes to the tool. This effort takes time and a certain level of expertise for the enterprise to maximize its benefit from its investment in the tool.
- **Impact on performance**—Because monitoring tools must operate in a manner that coexists with existing systems and data, it is important to understand the impact of a monitoring tool on base system performance and capacity. Embracing a monitoring tool that adversely impacts business processing capability is not sustainable in most enterprises.

If an existing operating tool can be leveraged to perform monitoring activities, there are fewer considerations to be made than when an enterprise is acquiring a new tool.

Task 4. Clarify reporting requirements and expectations.

Monitoring should be designed to confirm previously established expectations about the effectiveness of internal control and/or highlight identified deficiencies for possible corrective action. Generally, exceptions or deficiencies identified in the monitoring process are reported to the individual who is in a position to take corrective actions, as well as the person with overall responsibility for controls in a given area or for a given set of objectives. Because the controls being monitored often cross organizational objectives and business functions, one of the most important aspects of this activity is clearly defining how exceptions should be reported and to whom.

It is also worth noting that the process of correcting deficiencies may be considered to be a management activity rather than an element of internal control. Regardless of how it is classified, correcting control deficiencies should take place when the enterprise determines that control deficiencies are severe enough to warrant correction.

These attributes reinforce the need for the right people to receive the information necessary to enable corrective action to be taken and to allow management to provide sufficient oversight to gain assurance that the corrective action has been taken. COSO's 2009 guidance summarized several factors that may influence an enterprise's prioritization of identified exceptions and deficiencies, including:

- **The likelihood that the deficiency will result in an error or other adverse event**—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.
- **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 enterprise. The presence of such controls, when monitored, can provide support for reducing the severity of a deficiency.
- **The potential effect of a 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 factors listed previously, enterprises 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.

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

When analyzing a control failure resulting from monitoring or identifying where controls are needed as a result of the investigation of an operating problem or failure, those responsible for implementing controls should focus on root causes of problems. Two reliable tools to help determine root causes of failure include what is commonly referred to by experts as the "Five Whys," and a cause-and-effect diagram (also known as a "fishbone chart" or "Ishikawa diagram").

The "Five Whys" Approach

The "Five Whys" approach is a question-asking method used to explore the cause-and-effect relationships underlying a particular problem. In addition to helping identify the root cause of a problem, it can help clarify the relationship between different root causes of a problem or defect. Typically, it is most useful in addressing problems involving people and their interaction. An easy way to identify the root causes by using the "Five Whys" is to:

- Write down the specific problem. Writing the issue helps to formalize the problem and describe it completely.

- Ask why the problem happens and write the answer down after the problem.
- If the answer provided does not identify the root cause of the problem described in step 1, ask "why" again and write that answer down.
- Repeat s until the team is in agreement that the problem's root cause is identified. This iterative process may require asking "why" more or less than five times.

The example in **figure 8** shows the questions and answers for changes that have been made to production software without approvals. The root causes of the example turn out to be the lack of detailed user specifications and inadequate system testing.

Figure 8—Example Using the "Five Whys" Approach for a Control Failure

Question	Answer
Why were potentially uncollectible invoices not correctly factored into the quarterly analysis of the bad debt review?	The accounts receivable application improperly aged certain invoices.
Why did it only apply to certain invoices?	There was a data exception in a key field that is part of the aging.
Why were there bad data in the key field?	The specifications in the application change required by our new invoicing policies did not clearly define that blank is not allowed in the "invoice type" field.
Why was a blank allowed?	The application owner user did not define that the field could not be left blank.
Why was the situation not found during normal systems testing?	The requirements were not in the specifications.

Cause-and-Effect Diagram

A cause-and-effect diagram is generally used to explore all the potential or real causes (or inputs) that result in a single effect (or output). Causes are arranged according to their level of importance or detail, resulting in a depiction of relationships and hierarchy of events. A cause-and-effect diagram can help identify root causes as well as areas where there may be problems. It can also assist in comparing the relative importance of the different causes to ensure effective prioritization and coordination of remediation efforts.

To successfully build a cause and effect diagram:

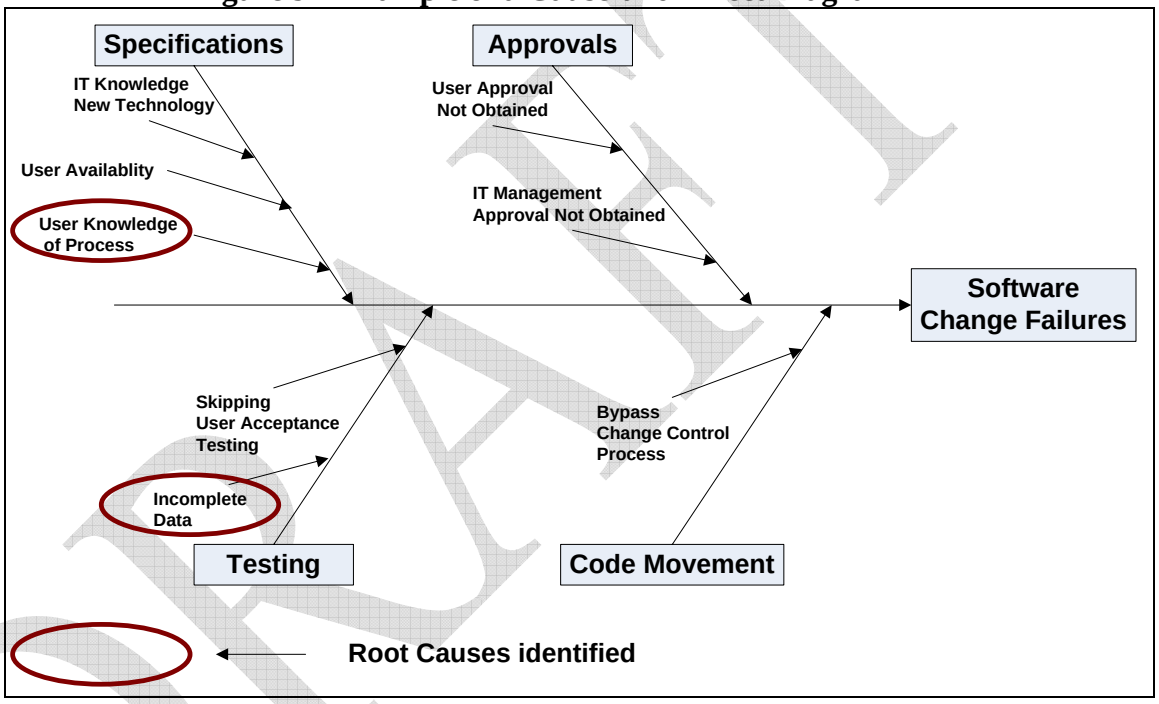
- Agree on the effect or problem statement before beginning:
- Identify major categories of failures. This may be equipment, policies, procedures and people for an IT process—but it can include other categories as well, depending on the circumstances of the environment.
- Link the potential or observed control failures to the categories.
- Discuss the control failure points with the project team.
- Revise the monitoring process and repeat testing as necessary.

When following the cause-and-effect diagram process, there are additional considerations, including the need to:

- Be concise.
- Think carefully about what could be its causes and add them to the tree for each node.
- Pursue each line of causality back to its root cause.
- Consider grafting relatively empty branches onto others or splitting up branches that become crowded.
- Identify which root causes are most likely to merit further investigation.

An example of a cause-and-effect diagram based in the failure of a software change is provided in **figure 9**.

Figure 9—Example of a Cause-and-Effect Diagram



Other Considerations Around Pervasive IT Processes

The IT-related controls and processes that were discussed previously largely focus on those activities that would either directly or indirectly relate to monitoring of business process-oriented controls. There are IT processes that support the control environment, risk assessment, and information and communication layers of the internal control framework. The following text summarizes the most pervasive of the IT processes that impact the internal control framework layers, along with examples of the questions that those providing oversight of the process need to evaluate in determining whether these controls are operating effectively.

IT Governance and Portfolio Management

Most IT organizations follow a planning process that is designed to ensure that IT is

aligned with organizational needs. Larger enterprises may have the "portfolio management" process that is designed to prioritize the utilization of those IT applications and other resources that are of most value to the business. There may also be an IT governance process that defines how decisions will be made and communicated. Those providing oversight need to ensure that the most critical questions are being addressed, including:

- Does IT have an effective process by which managers participate in establishing organizational objectives and resolving conflicts and disagreements?
- Does the IT organization have an effective method of defining and aligning specific plans, tactics and resources required to achieve accounting and financial reporting objectives?
- Does IT management communicate its strategies, activities, challenges and risks on a regular basis with the CEO and CFO, and, to the extent necessary, the board of directors?
- Is the IT organizational structure sufficient to provide for necessary information flow to manage its activities?
- Are roles and responsibilities of the IT organization defined and understood?
- How is the need for new or changed IT policies, defined, vetted and approved within IT and at the organizational level?
- Does IT staff understand and accept their responsibility regarding internal control?

IT Risk Management

An IT organization should have a process whereby it evaluates its risks. This activity could be done on a stand-alone basis for IT or it could be part of an enterprisewide risk management effort. These activities may be done through formal, structured processes or they may be done through an extension of existing management, planning or governance processes. The form of the activities is less important than their substance. Those providing oversight need to ensure that the most critical questions are being addressed, including:

- Does IT management have effective methods to identify and react to changes that can have an impact on IT controls?
- Does the IT organization have a risk assessment framework that is used periodically to assess risk that would impact financial reporting objectives?
- Does the IT organization have an effective method of communicating internal control and fraud prevention objectives and expectations to all relevant personnel?
- Does IT management respond effectively to operational and control deficiencies identified through internal audits or the reports of independent third parties (including external auditors)?
- Are significant IT events or failures, e.g., security breaches, systemic-based fraud, major system failures or internal control weaknesses, investigated, resolved and reported to senior management or the board, as required?

In enterprises wishing to enhance the maturity of risk management practices, *The Risk IT Practitioner Guide*[4] can provide a solution accelerator, not in a prescriptive manner but as a solid platform upon which an improved practice can be built. *The Risk IT Practitioner Guide* can be used to assist with setting up an IT risk management framework in the enterprise, as well as enhance existing IT risk management practices.

Monitoring

Finally, because monitoring is part of a system of internal control, the monitoring process itself should be reviewed regularly to help ensure that the monitoring process continues to operate effectively. Volume I of COSO's 2009 guidance provides the following starting set of questions to be considered when evaluating the monitoring process. Although these were defined for the enterprise as a whole, they are equally applicable to the IT-related monitoring activities.

Effectiveness

1. Has the enterprise appropriately considered all of the risks that could materially affect its objectives?
2. What recent changes have taken place within the enterprise's environment, people, processes or technology, and did the enterprise 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 enterprise discussed, at an appropriate level of detail, the risks the enterprise 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 enterprise'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 enterprise about the effectiveness of monitoring?
6. Have the internal or external auditors uncovered control deficiencies not identified by monitoring?
7. Is there a process for tracking control deficiencies through evaluation and remediation?
8. Have all identified deficiencies been addressed properly?

Efficiency

1. Is the enterprise monitoring controls at a cost, effort or organizational level that is inconsistent with the amount of risk the controls mitigate?
2. Is the enterprise monitoring internal controls in areas that have never had a control failure and have not been known to cause errors in similar enterprises? (Note: this may not be a reason to omit monitoring procedures, but it may affect the desired type, timing and extent of monitoring, including the organizational level at which monitoring might be performed.)

[4] ISACA, *The Risk IT Practitioner Guide*, USA, 2009, *www.isaca.org/riskit*

3. Do risk areas exist within the enterprise that rarely experience meaningful change and that, 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)?
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?

Addendum—Additional Guidance for IT Professionals on Implementing a Monitoring Approach

This addendum has been developed to provide additional guidance to IT professionals by including a further discussion and approaches to executing an IT monitoring project, along with sample templates that practitioners may find useful. As noted in the chapter, the four-step process is not a rigid, sequential process, and this addendum further illustrates that concept by taking a project-based approach to developing and executing a monitoring program.

Step 1. Prioritize risks.

One of the challenges IT professionals may face, when being involved in a monitoring project, is to broaden the scope of the risk assessment from just being an IT risk assessment to being a business risk assessment. This requires focusing on IT processes to determining how the business may be affected by internal and external IT risk factors.

This involves:

- Understanding each business process and the role IT plays in that process, and
- Understanding the business objectives, related risks and key controls associated with the business process

Asking and answering questions such as the following can facilitate the IT professional's understanding of the business process and the internal control environment:

- What is the objective of the business process?
- When and how does the process start? Is there only one way—or are there many? Have the other ways been identified? What are the triggers?
- How does the process end?
- Is the process defined in terms of steps or activities that lead to the predicted outcome?
- Which process steps or control activities are automated? Which ones are performed manually? Who performs the manual control activities?
- How is success measured? Do the metrics cover the essential parameters to determine whether the objective is being met? These include parameters such as:
  - **Effectiveness**—Does it meet the output criteria (i.e., deliver what was ordered) with the promised quality, timeliness?
  - **Efficiency**—Are resources managed well?
  - **Accuracy**—Does it meet specifications?
  - **Other key factors—**Are security, timeliness, confidentiality, integrity, availability, compliance and reliability addressed?
- Who is responsible for the process performance? Can the accountable process participants and their related roles in the process be identified?
- What other materials or information are utilized in the process?

- Are significant risks identified and prioritized?
- Are control activities defined to address higher priority risks?

Risks should be considered in the context of organizational/business objectives so they may be prioritized and appropriate resources allocated to manage them. A formal risk assessment can identify and evaluate the full range of risks against the stated business objectives and the unique control environment of the enterprise. It also can highlight functional areas that are most likely to impact enterprise objectives so that management can make informed choices. No enterprise has unlimited resources. Information, people, applications and infrastructure allocated to reduce risk in one area inherently detract from resources that could be employed in other, potentially higher-risk areas.

Steps 2 and 3. Identify controls and information.

As was mentioned earlier in this section, key controls that address meaningful risks are the preferred candidates for monitoring because of their relative importance. If the business objective is important and the risk is high, a related key control should be monitored, regardless of the nature of the control or the size of the IT department, based on a cost-benefit analysis. By selecting "key controls" that address "meaningful risks," management can efficiently focus its limited resources on high-value control activities. When selecting key controls, specific considerations for the IT professional include:

- Key controls that are IT dependent usually are dependent on selected IT general controls.
- The risk assessment process and the availability of computerized information drive which IT and manual controls will be monitored.
- Information needed for monitoring may be available only from an IT process.
- Monitoring of IT controls and automated monitoring often can be leveraged to address multiple monitoring objectives.
- When key controls are IT dependent, underlying IT general controls need to be monitored.
- It facilitates a repetitive, and often a continuous, monitoring process.

Figure 10 describes considerations relating to the complexity and maturity of business and IT process control types.

Figure 10—Business and IT Process Control Types and Considerations

Process Criteria	Considerations
More complex	Use existing process documentation methodologies, such as Six Sigma Suppliers, Inputs, Process, Outputs, Customers (SIPOC), to identify controls that may benefit from monitoring. See appendix C.
Less complex (mature, routine, or not complex)	Select monitoring activities that can be leveraged across multiple controls. Use existing technology or off-the-shelf tools for monitoring controls with minimal investment.
More mature	Integrate control monitoring into the daily business process operations

Figure 10—Business and IT Process Control Types and Considerations	
Process Criteria	**Considerations**
(well defined and managed)	(and the business process documentation) to add value.
Less mature	Once a control baseline is established, implement more frequent and stringent monitoring of the control until a control baseline is established.

Broad monitoring coverage for *all* key controls can be achieved by using a combination of direct and indirect information sources. However, in addition to the factors discussed in this chapter, the monitoring depth and frequency of *specific* key controls can be further determined by considering the following:

- How directly does the control support the relevant business objectives?
- What risks does the control address and how important are they?
- Is the control considered a key control?
- What are the feasibility and cost of monitoring the control (using either direct or indirect information)?
- What is the nature of the control? Is it manual or automated, detective or preventive? If manual, is it dependent on IT information or an IT process for its effectiveness?
- If historical data are available, what is known about the maturity and past operating effectiveness of the control?

Once these factors are considered, the process of identifying the controls to be monitored and the information source for monitoring (direct or indirect) can begin. The following actions should be taken:

- **Identify controls that are in scope for monitoring—**Although key controls should be monitored, the degree of monitoring may vary based upon relative risk and value of each control. For example, those controls that address important risks related to the most important business objectives and those that support multiple objectives might be monitored more extensively.
- **Determine the information sources available for monitoring—**As **figure 7** indicates, direct information is more effective than the use of indirect information in ongoing monitoring and usually allows for fewer separate evaluations. However, in addition to direct information, indirect information such as key performance indicators (KPIs) may be useful. Performance indicators found in ISACA's COBIT framework can provide an excellent source for determining potential indirect monitoring measures.

In short, the management team expects that its most important processes will be both well defined and tightly controlled. However, the rigor of managing and measuring a process can vary—and depends greatly on how the enterprise interprets the relative importance of one process in comparison to others.

Step 4. Implement monitoring.

Implementing a monitoring program begins with the development of a project plan. To help ensure that monitoring project is successful, the plan should consider the

attributes shown in **figure 11**.

Figure 11—Attributes of a Monitoring Project Plan
Business case—Describes the benefits for undertaking a monitoring project. Why is this monitoring project important to the enterprise? What are the risk implications of the failure of key control(s) selected for monitoring? Why is it important to do it now? How does the monitoring project align with enterprise goals? What are the consequences of *not* doing this monitoring for the enterprise?
Problem/opportunity statement—States what problems or needs the initiative will solve. Clarifies the "why" of undertaking the project. Example: Control failures within the software change management process can result in processing errors and other control failures affecting enterprise operations and make excessive programming rework necessary within the IT department.
Goal statement—Defines the objective of the project in measurable terms. The goal statement should solve the potential problems identified in the problem/opportunity statement. It provides direction for detecting control failures, leading toward solutions. Example: Monitoring of key controls within the change management process—specifically, the use of formal change request forms, approval of change requests by authorized personnel, and testing of all changes in compliance with enterprise policy—will increase system reliability and help availability, decrease rework and help contain cost.
Scope—Defines the boundaries of the project and should answer the following types of questions: • What parts of the enterprise or business processes are included in the scope? • Where will the work be performed? • What parts of the enterprise or business processes are *not* included in the scope? • What is the role of IT and users in this project? • Can the project be subdivided so that a pilot area can be reviewed first to test the: – Assumptions – Data collection – Testing processes
Approach—Defines the information, methods and tools selected for the monitoring projects. The type of sampling may also be documented.
Time line—Documents the major milestones and timing for the project. As a minimum, the plan should consider the time for the design, implementation, testing and periodic follow-up on results.
Project team—Identifies the monitoring team. The team members should include people with good knowledge of the business process. They should have IT skills that enable them to understand the IT processes and IT controls. If specialized IT automated audit tools are required to obtain sample transactions for review, someone on the team needs to have the skills and experience to develop the automated testing process.
Persons accountable and responsible—Identifies the senior management personnel who are accountable for the monitoring project; also identifies the leaders of the monitoring project and key members of the business process teams involved in the monitoring

Once the project plan has been developed, the process of determining the frequency for monitoring, developing the monitoring procedures, and determining thresholds for monitoring that utilize indirect information can begin. The following actions should be taken:

- **Determine the frequency for monitoring—**A determination must be made regarding the use of ongoing monitoring or separate evaluation techniques.

When ongoing techniques utilize highly persuasive information (i.e., direct information), they can routinely provide evidence that a control is operating as intended. If they use less persuasive information (i.e., indirect information), additional separate evaluations may be required more frequently. In both cases separate evaluations may be required periodically.

Automation is another consideration in determining the frequency of monitoring. In general, automated controls require less frequent monitoring of their automated aspects because once the control is verified to be working properly, automated aspects are unlikely to change unless change management controls within the system cannot be relied upon. Nonautomated aspects, such as follow-up on reported exceptions, may require more frequent monitoring, depending on the risks. An automated control may allow for even greater usage of indirect information, once the initial baseline using direct information has been established, as system controls are less likely to degenerate than manual controls if—**and only if**—the underlying IT general controls are effective.

- **Develop monitoring procedures—**A monitoring procedure needs to be developed for both ongoing and separate evaluations. The project plan should specify the information source to be utilized for each approach. Enterprises using indirect information as a source for ongoing monitoring will still find it necessary to perform a separate evaluation using more persuasive or direct information. In addition, monitoring procedures that provide comfort over more than one control may be given preference over more targeted procedures (e.g., the review of a change control ticket may provide evidence of business sign-off, testing results and the existence of a back-out plan).
- **Determine thresholds for monitoring that utilize indirect information—** Indirect information cannot provide positive assurance that a control is operating effectively. However, indirect information can be a good indicator of the effectiveness with which the process meets its overall performance objectives. If such indirect information suggests that the performance objectives are not being met, this may indicate that the related key controls are not functioning effectively. A tolerance window for the deterioration of a key metric or indirect monitoring should be established to trigger the need for direct monitoring or other follow-up action.

Figure 12 provides an illustration of how the decisions made in steps 2 through 4 can be consolidated and documented. It has been completed with an example using IT general controls for a software change control process.

Figure 12—Control Information Grid

Control	Key (Yes/ No)	Nature of the Control	Direct Documentation Source	Direct Monitoring Approach	Indirect Information	Indirect Monitoring Approach	Monitoring Threshold (Trigger)
All changes to production require an electronic change request. Emergency changes may be documented after the change but within 24 hours.	Yes	Automated/ detective	Changed files/ library reports Service desk tickets Service desk change logs	Each month the changed object report is reconciled against the request for change (RFC) record. This is performed using an automated correlation engine [5] and an exception report is generated, which is reviewed and followed up.	Availability reports, including number of emergency changes to production systems	Each week availability data are reviewed along with a report on the number of emergency changes.	Trend data that indicate a decrease in availability by 1 percent or more, or an increase of emergency changes by 5 percent or more result in an immediate execution of direct monitoring.
All change requests must be approved by the business application owner prior to moving into production.	Yes	Manual/ detective	Service desk RFC records	On an annual basis a sample of RFCs is selected and reviewed for appropriate business owner approval prior to release into the production environment.	Availability reports, including number of emergency changes to production systems	Each week availability data are reviewed along with a report on the number of emergency changes.	Trend data that indicate a decrease in availability by 1 percent or more, or an increase of emergency changes by 5 percent or more result in an immediate execution of direct monitoring.

To be successful, sponsors/control owners need to be able to rely on the monitoring process itself for reliable results. Consequently their involvement is essential during the development process and once the monitoring process is operational.

To ensure correct results and conclusions, the monitoring process must be repeatable and minimize the variations in how monitoring is performed. In cases where a monitoring process is critical to an enterprise, it may be necessary to implement controls over the monitoring process itself to detect and manage variability in how the data are extracted, validated, analyzed and reported.[6]

[5] A correlation engine is an intelligent processing unit that contains business rules and assesses events before an event trigger is generated, which determines the response selection for the specific event.

[6] An analytically based process is available to help ensure the accuracy of monitoring. Measurement Systems Analysis (MSA) is a Six Sigma-based process for analyzing the monitoring processes for potential variation and

Automated monitoring is less likely than manual monitoring to produce variations in the monitoring processes. As stated previously, effective IT general controls must be in place for development and subsequent operation of automated monitoring solutions. These include controls over software development, software maintenance, and system and user testing. Such controls are covered in detail in various ISACA publications, such as COBIT, Val IT and the *IT Assurance Guide*.

After a monitoring project is complete and the system is operational, processes need to be in place to monitor and assess the results. Although testing would have been performed to validate the functionality during development, ongoing activity that needs to be considered includes:

- Reviewing the monitoring results to minimize false positives or negatives and ensure valid, current and timely results. Control failures may be reported when, in fact, they are not failures because the business itself has changed. This would be more likely to be true with continuous controls monitoring solutions vs. manual monitoring processes.
- Determining the reason for the control failure
- Reporting results back to the project sponsors, along with any recommendations, so they can implement corrective actions

Once the monitoring process flags a potential control failure, identifying the root cause will aid in defining appropriate corrective actions. The goals of root cause analysis are to identify and correct the primary reason for the failure of the controls. More information may need to be gathered, such as when, where and how the failure occurred. Did it occur because of a recurring condition that could be resolved by process improvements, or is it due to a less common or special circumstance that would have been difficult to predict or anticipate? Further testing or sampling may be required to determine if the failure is repeated. Two tools were discussed in this chapter to help determine root causes of failure, namely the “Five Whys” and a cause-and-effect diagram (also known as a “fishbone chart” or “Ishikawa diagram”).

It is important to identify the appropriate levels of enterprise management that must be informed about the condition or event, the type of corrective action that is or will be taken, and the expected time frame for mitigation (assuming it is not post-recovery). Management should receive information that is clear and concise (preferably stated in nontechnical business terms) to enable efficient and effective understanding of the impact to the enterprise and clients.

As a minimum for reporting, the results of monitoring should include the items listed in **figure 13**.

defects. For further information on how to create and use an MSA process, refer to a Six Sigma Black Belt resource in your enterprise or to web sites such as *iSixSigma.com*.

Figure 13—Items to Include in a Report on Monitoring Results
Problem statement—Identify the problem, e.g., control failure.
Cause identification—Describe the cause of the control failure.
Perspective on risk—Describe the risk to the business process created by the control failure. For example, the risk might be lack of compliance with a particular standard or regulatory requirement. Also describe any adverse consequences that may have occurred.
Recommendations—Identify the corrective action, including what is to be done, by whom and by when (estimated completion date). Any follow-up actions should also be discussed.

Any warranted and cost-justifiable changes should be noted and any changes resulting from corrective actions taken should be mapped back to any processes affected. Documentation should be updated and appropriate personnel notified. Also, the monitoring process should be regularly reviewed to help ensure that the monitoring process itself, as well as the controls it monitors, continues to operate effectively.

Case Study: Alpha-Bravo Company

The Alpha-Bravo case study illustrates the concepts for the design and execution of a project to monitor IT controls. It features a company that implemented an IT monitoring activity to address a business problem. Although normally monitoring processes would be implemented to monitor controls that are believed to be operating effectively, this illustrates an approach of how monitoring might be used to help determine the root cause behind ineffective controls.

I. Scenario

Alpha-Bravo Company is a specialty electronics manufacturing enterprise that customizes products for customers. Alpha-Bravo has been experiencing large inventory variances and customer returns, which were due to the wrong products being shipped.

The shipping system creates invoices, which accompany shipments. It also creates special pick lists for picking the products from the warehouse.

Alpha-Bravo's shipping and billing system has been created and maintained in-house. The warehouse, product picking and shipping processes are highly automated and Alpha Bravo does not deem it practical to add manual control procedures. The system is considered significant and contains a number of key controls for financial reporting. Therefore, it is reviewed and tested annually in preparation for the financial controls audit. This financial controls pre-audit process identifies the key controls for the shipping process, and the audit process is supported by process documentation.

Recently, the system has experienced many system failures and the IT department, under pressure to keep the system in operation, has been making many changes.

The Controller is very concerned about the internal controls over shipments. He wants the IT department to ensure that all changes to the shipping system are approved and properly tested prior to implementation.

II. Designing a Monitoring Program

The controller assigns Alpha Bravo's IT business process analyst James and the IT manager Igor to implement effective controls in the software change management process as well as monitoring activities to ensure that key controls within the process remain effective over time.

From existing process documentation, James finds that IT uses more than one change control process, depending on the infrastructure and operating system used.

To manage the project, James works with Igor to create a project plan, as shown in **figure 14**.

Figure 14—Alpha-Bravo Project Plan

Business Case
The shipping/billing system and related processes are key to Alpha-Bravo's business. Through prior project indirect monitoring, the business staff believes the issues are caused by failures in IT software change control procedures. Continued failures in the shipping and billing process could result in the loss of significant sales. The shipping, billing and IT change control processes are in the scope of the annual financial compliance pre-audit. The next financial compliance pre-audit will not be performed for nine months.

Opportunity Statement
- Shipments are not always correct.
- Key software change controls may fail, e.g., software changes for the shipping/billing systems may not all be approved by both the business operations manager and IT director, and software changes may not be tested using the specified testing process.
- It is not deemed practical to add further manual controls to the shipping process.

Goal Statement
- Identify and validate the root cause of incorrect shipments
- Establish a monitoring procedure to collect all shipping system change requests on a weekly basis to verify approvals.

Scope
- Includes all changes to the shipping/billing system
- Review of other applications should be limited to constrain the scope of this monitoring project.

Approach
- Analyze existing software change process to identify control gaps
- Design and implement cost-effective controls to ensure that only approved changes are introduced to the production environment.
- Implement monitoring activities to ensure that key software change controls remain effective over time, leveraging existing resources.
- Review all changes to the shipping/billing system.
- Interview the appropriate IT and business staff.

Figure 14—Alpha-Bravo Project Plan
Time Line • Plan & Organize • (Acquire) & Implement • Deliver & Support • Monitor & Evaluate – Initially, the monitoring results will be provided to the IT manager and financial controller on a weekly basis; once monitoring results indicate the process is adequately controlled, monitoring will continue but the reporting will be changed to occur on a monthly basis.
Project Team • An IT business analyst is assigned to collect change requests and test results daily. • A technical analyst is assigned to create a report of changes from the application library log. • The warehouse supervisor is assigned to provide any observed changes in the shipping system.
Persons Accountable and Responsible • The IT manager is accountable for the change control process. • The controller is the sponsor of the project.

Before starting the monitoring project, the controller, who is the project sponsor, must agree to the project plan. The cooperation of the IT manager is also needed. The IT manager should agree with the plan and provide staffing and technical support to gather the documentation to review for monitoring.

III. Findings, Root Cause and Corrective Actions

The following are the findings, root cause and corrective action:

- From the results of the first week of testing, James finds that:
  - Changes are not consistently approved.
  - Key application controls that link customers to orders were not included in testing.
- Through further analysis of the change process, James finds that the operations manager was not included in the change request routing. Additionally, there were no written requirements to test customer linkage controls during each software update.
- The workflow for approving changes was modified to incorporate appropriate management approval. Testing processes were changed to make sure that key controls were included.

IV. Results

With only minimal investment from the Alpha-Bravo Company, the monitoring process has helped identify and remediate the root cause of incorrect shipping labels and continuous monitoring has significantly improved shipping accuracy for improved customer satisfaction. The monitoring process continues on an ongoing basis and the financial pre-audits have not identified new problems.

4. How to Automate Monitoring of Controls to Increase Efficiency and Effectiveness

Automation is more than just a highly efficient and effective way to capture the benefits of monitoring. It can also deliver an additional "premium" level of benefits to the enterprise—often, but not always.

Do your homework. Understand the costs and benefits.

Map the options to your unique set of circumstances.

This chapter discusses automating monitoring activities—including the use of tools to facilitate the process and integrating the automated monitoring of controls with other automated monitoring processes for increased efficiency and effectiveness.

COSO Volume II monitoring guidance discusses two categories of automated monitoring tools. They are control monitoring tools and process management tools. The first category, control monitoring tools, generally is the one that involves more development effort as they are used to perform routine tests and often will enhance the effectiveness, efficiency and timeliness of monitoring specific controls. 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.

Control Monitoring Tools

As noted by the COSO guidance, many automated control monitoring tools 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. As noted in chapter 3, monitoring tools typically focus on one or more of the following:

- **Transaction data**—Comparing processed transaction (or masterfile) data against a set of control rules established to highlight exceptions and/or identify instances in which the controls over a process or system are not working as intended
- **Conditions**—Examining application or infrastructure configuration settings/parameters and comparing them with a baseline or with previously established expectations. An example could include tools that monitor system access controls.
- **Changes**—Identifying and reporting changes to critical resources, data or information, making it possible to verify that changes are appropriate and authorized
- **Processing integrity**—Verifying and monitoring the completeness and accuracy of data as they progress 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

Process Management Tools

Many of the process management tools use workflow techniques to provide structure and consistency to the performance and reporting of monitoring

procedures. Some features that make these tools useful include their ability to:

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

The remainder of this chapter will focus primarily on control monitoring tools, given the need to integrate the tools and techniques into the business processes.

Understanding the Benefits and Challenges of Automated Monitoring Tools

When used effectively, the aforementioned tools help turn data into meaningful and timely information, which provides valuable insights and drives better decision making. Automated monitoring of control and business process effectiveness and efficiency can help the enterprise refine its existing business processes and identify cost savings and potential cost recoveries. Ultimately, automated monitoring facilitates a more comprehensive internal control system and quality audits while decreasing risk, and provides an opportunity to increase return on investment (ROI).

Automated monitoring of controls may help:

- Reduce effort and cost while increasing process efficiency and control effectiveness.
- Enhance the effectiveness of line manager/staff with internal control compliance efforts.
- Provide real-time information for proactive preventive measures.
- Leverage real-time information and compliance investment for business value generation.
- Provide a sustainable and repeatable process to enable data and control quality improvement.
- Create a perception of detection to deter fraud.

In addition, automation can significantly enhance the monitoring process through:

- **Profiling and data stratification**—Automated tools can help identify and analyze focus areas of risk by segmenting large amounts of data into areas of interest.
- **Trending**—Automation can help trend data over time to identify control effectiveness changes.

- **Customized transactional analysis**—Automated tools facilitate data analysis geared toward specific business processes (e.g., financial reporting, accounts payable, accounts receivable, inventory and human resources).
- **Scalability and portability**—Monitoring scripts and scenarios can often be transferred from one business process to others.
- **Identifying activities that may circumvent existing controls—**Anomalies and "red flags" related to specific fraud schemes can be identified by using enhanced logic and algorithms, such as Benford's law.[7]

Even though the benefits of automated monitoring may be great, there are numerous challenges to achieving these benefits. Because the task seems overwhelming, enterprises may hesitate to implement automated monitoring, citing factors such as:

- IT environments are increasingly complex, with many diverse systems and data owners.
- Key controls suitable for automated monitoring are difficult to identify or seem part of the "IT shop."
- Data seem overabundant and distributed across separate systems.
- Persuasive information appears difficult to identify.
- The process of data extraction and analysis is arduous.
- The benefits may not be apparent.

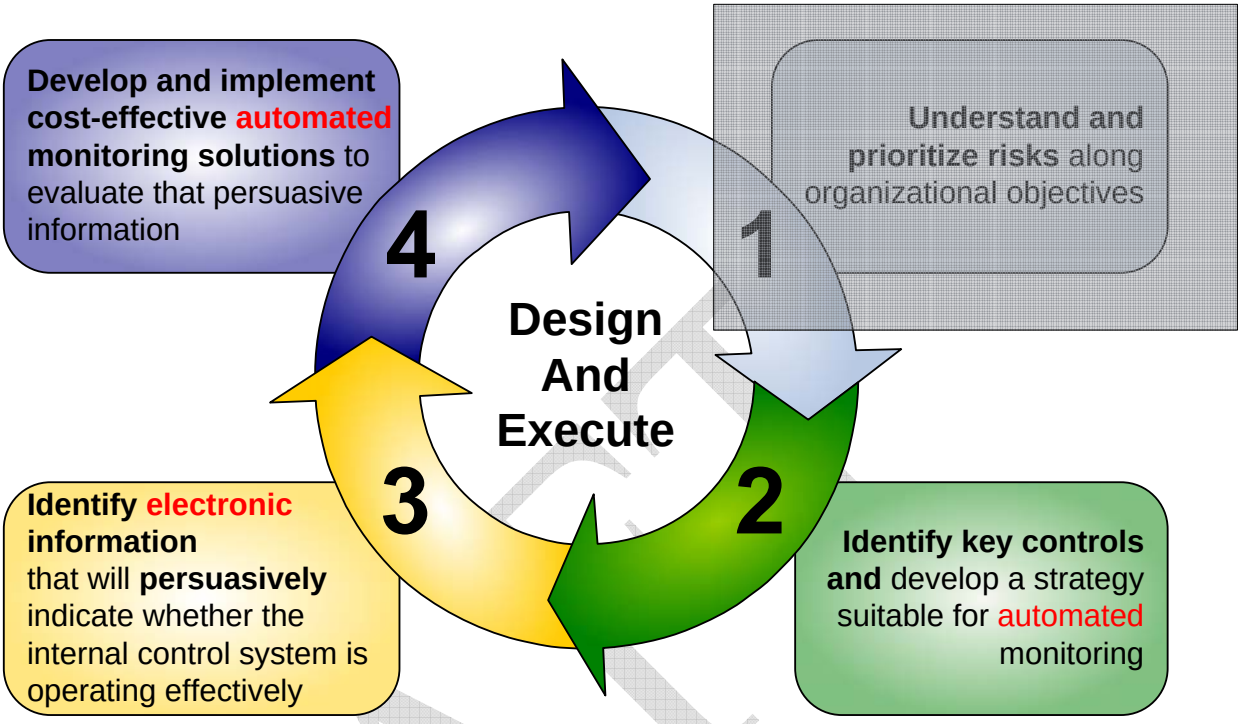
Even enterprises that already perform some basic data analysis may not see a clearly apparent value proposition for implementing automated monitoring processes. This may be a result of *ad hoc* testing of control effectiveness instead of setting up a *repeatable* process for measuring the effectiveness of controls over time.

What follows is a more in-depth discussion for identifying key controls suitable for automated monitoring. Once an enterprise decides to embark on a project to automate the monitoring of controls, many of the steps described in chapter 3 are applicable.

Enterprises confronting these challenges may find it helpful to follow a sequenced series of steps—a road map—to automate the monitoring of controls (**figure 15**). Since step 1—Understand and prioritize risks along organizational objectives—would not change from what was discussed in chapter 3, this section will focus on additional considerations for steps 2, 3 and 4.

[7] Benford's law, named after physicist Frank Benford, states that in lists of numbers from many (but not all) real-life sources of data, the leading digit is distributed in a specific, non-uniform way. According to this law, the first digit is 1 almost one third of the time, and larger digits occur as the leading digit with lower and lower frequency, to the point where 9 as a first digit occurs less than one time in twenty. This distribution of first digits arises logically whenever a set of values is distributed logarithmically.

Figure 15—Road Map for Automating the Monitoring Process



Each of the remaining three steps is addressed in more detail in the following sections.

Identifying Key Controls and Developing Strategies Suitable for Automated Monitoring

Chapter 3 discussed selecting controls from either an application or general perspective. The discussion that follows here focuses on four broad types of key controls to illustrate how application and general controls are often integrated:

- IT inherent
- IT configurable
- IT-dependent manual
- Manual

IT Inherent Controls

Inherent controls are those designed and built into a system by the vendor or, in the case of a system developed in-house, by the software development team. As such, they *cannot* be easily altered after system implementation. They are often hard-coded and can be considered stable and reliable in environments where effective software development and change management processes exist.

Examples of inherent controls[8] are:

- Edits, validations and exception reports that are hard-coded into the IT application
- Business process workflows
- Files and tables used for processing (standard tables)
- Automated process completion checks
- Programs that govern system access
- Built-in system features that provide control benefits, such as the requirement for debits to equal credits in an accounting system or the inability to post sales transactions to non-sales expense accounts

Testing of Inherent Controls to Establish a Baseline

Since inherent controls are those files, tables, processes, reports and data that exist as part of the standard application configuration, they are generally tested during system implementation as part of user acceptance. Original system implementation testing can provide a baseline of key controls against which to measure for future testing. If the system is already in production, enterprises may have to establish a baseline for individual key controls.

Once the baseline is established, ongoing monitoring of changes to the system can provide assurance that the inherent controls are continuing to function effectively. Such monitoring should ensure that:

- Only authorized individuals can make changes to the system.
- All changes are approved, tested and accepted by the system owner.
- Controls that may be affected by the change continue to function effectively.

Periodically, separate evaluation may be necessary depending on the nature and frequency of system changes and the risk assessment.

Automated Monitoring of Inherent Controls

As mentioned previously, monitoring of inherent controls relies heavily on the software development/implementation and change management controls.

Monitoring of inherent controls, therefore, occurs after system implementation by monitoring the change management process. Automated change management tools and utilities can be leveraged to identify all system changes. Identified changes are then compared to the change request and approval log to ensure that the change management process was followed and controls were not circumvented. Exceptions to the process are flagged for management review and follow-up.

An additional consideration is monitoring changes that might not go through the normal change management process, such as file restores or patch management.

[8] These are examples only; actual classification depends on the enterprise's control practices, including acquisition vs. in-house development and how files and tables have been implemented.

IT Configurable Controls

Configurable controls are those that allow the user to update, change or enable/ disable the operation of a control that is built into an IT application or process, without making programming changes. Configurable control settings are generally contained in configuration tables. Many financial, manufacturing and infrastructure systems use configuration tables to give application users flexibility to customize the application or system to their specific needs. Configuration settings may also allow users to change the overall workflow of an application or system to enable or disable embedded functionality.

Examples of configurable controls are:

- Edit and validation tables and files
- Criteria and rules for producing exception or management reports
- Security profiles for sign-on access
- Segregation of duties by controlling access to screens or specific fields
- Changes to business and reporting organizational structures in the application system, such as adding or removing a segment of a business structure

Testing of Configurable Controls to Establish a Baseline

The key differentiator between inherent and configurable controls is that inherent controls are designed so they *cannot* be altered after system implementation, whereas configurable controls allow for easy customization (without changing the system) for different business units with unique requirements. This can provide a high degree of flexibility across entities of an enterprise that operate in different countries, industries, etc. The baseline for configurable controls can be established as part of user acceptance testing during system development and prior to implementation. If the system is already in production, a separate evaluation of key control settings and their operation may be required.

Automated Monitoring of Key Configurable Controls

Appropriate tools and techniques for monitoring configurable controls include:

- Leveraging and expanding the activity described for monitoring inherent controls to include monitoring changes to configurable controls
- Generating a report of current configuration settings and capturing management's agreement/updates to the settings in an electronic log file
- Periodically comparing the current configuration settings to the prior scan. Any changes would be reviewed to determine if the change control process was followed.

IT-dependent Manual Controls

Many controls in IT applications require manual review or manual intervention to ensure proper operation. For the purposes of this publication, IT-dependent manual controls are defined as those steps or processes performed by people as part of a control process, using information provided by an IT application or system.

The effectiveness of IT-dependent manual controls relies on the effectiveness of both the underlying IT process and the manual control activity. The IT process may have inherent/configurable control attributes, as discussed previously.

Examples of IT-dependent manual controls are:

- Follow-up on system exception reports
- Balancing of transaction counts and values between interfaced systems
- Management review of hash totals
- Review of system logs
- User input controls that show completeness of processing, such as reconciling beginning and ending balances based on user transactions

Testing of IT-dependent Manual Controls to Establish a Baseline
Establishing a baseline for the IT inherent and configurable aspects of the control was discussed previously. Since establishing a baseline for the manual aspect of the control is the same as for manual controls, it is covered as part of the following manual controls discussion.

Automated Monitoring of IT-dependent Manual Controls
Automated monitoring of the IT inherent and configurable aspects of the control was discussed previously. Automation opportunities for manual controls are discussed in the section immediately following.

Manual Controls

Manual controls are those controls that are independent of IT processes. Manual controls are often workflow steps performed by people, such as inquiry, observation, exception handling or performance. Since the control procedures are not IT-based, automation of monitoring often is not feasible. However, there may be instances in which automation can still be leveraged.

Testing of Manual Controls to Establish a Baseline
Since manual controls rely on people to perform the control activity, there are additional considerations relative to its performance, such as timeliness, accuracy and completeness. For example, did the individual complete the control activity in a timely manner? If the control activity was performance-based, was it done accurately?

Establishing a reliable baseline for manual controls cannot be approached in the same manner as IT inherent or configurable controls. Rather, reliance is often obtained by performing separate evaluations to include reperformance, self-assessments, internal audit and management oversight—activities that provide opportunities for automation.

Automated Monitoring of Manual Controls

Since the control is manual, the opportunity for automation may be the automation of the log that captures if and when the control was performed, who performed it, and whether exceptions were followed up and addressed. Using the example of bank reconciliations, the person performing the reconciliation would enter into a log that the bank reconciliation was completed, along with the completion date. This log could then be reviewed to provide assurance that the bank reconciliation was completed in a timely manner. To the extent exceptions were identified, resolution and follow-up of the exceptions could also be noted in the log file for review and assurance that follow-up did occur on a timely basis.

Strategies for Automated Monitoring of Key Controls

When determining how best to leverage automation to monitor key controls, it is helpful to determine an overall strategy that will ensure the most effective and efficient monitoring approach. This section is intended to help determine a monitoring strategy, based on the enterprise's level of control automation.

Figure 16 is a worksheet that may prove helpful in working through the strategy development process.

Figure 16—Key Controls and Control Type

Key Controls	IT Inherent	IT Configurable	IT-dependent Manual	Manual	Comments
E.g., review of aging report	*X*		*X*		
E.g., three-way match	*X*	*X*			*Rely on IT inherent control*

The worksheet is used to capture all the key controls. As each control is entered on the worksheet, it is classified as to its control type: IT inherent, IT configurable, IT-dependent manual or manual. One control may have several classifications (e.g., the review of an aging report). The IT inherent control type is checked because the aging categories were hard-coded into the aging program vs. being configurable. The IT-dependent manual control column is also checked since the control includes a review of the aging report by someone in the accounts receivable department who is responsible for ensuring that appropriate follow-up action is taken.

The completed table will help the enterprise determine the monitoring strategy that will provide the greatest cost-benefit and leverage.

If the number of IT inherent controls is large, monitoring activities targeting key controls within the application system development and change management processes may be the most efficient and effective ones to automate. Monitoring may consist of an automated routine to detect changes to programs containing key control logic or parameters. Once the automated routine is developed for one system, it can most likely be leveraged across all systems using the same system development and change management processes. Such similarities can be noted in the Comments column of the spreadsheet.

Developing monitoring activities over IT configurable controls may be more system-specific and focused than monitoring IT inherent controls. In the aging report example, assume the aging categories are based upon configuration settings contained in a table that can be changed outside the program change management process. Also, the table in which the configurable categories are maintained is used only by the accounts receivable system. A strategy for automating the monitoring of such configurable controls must take into account the added consideration of who is authorized to make changes. If the configurable controls being monitored are maintained by the IT department, there may be leverage from system change-control activities around monitoring IT inherent controls since similar controls may be applicable. An additional requirement may be a need to develop an automated routine to detect changes to the tables containing the configuration values instead of leveraging the routine developed above to detect changes to programs. (Assurance required about the continued effectiveness of IT inherent controls that support the configurable controls can be obtained using the monitoring activity over change management discussed previously. This should eliminate any need to perform additional monitoring activities over IT inherent controls.)

If the configurable tables are maintained by user departments, the monitoring activity may be more directed to that department, not providing as much leverage as monitoring activities by the IT department. An approach to automated monitoring for a user-managed configurable control might be to establish a baseline of the configuration settings and periodically run a routine that compares the baseline against current settings. If the settings have not changed, no further action would be required. If there were changes, a determination could be made as to the appropriateness of the changes and whether they were approved. Regardless of the approach used, it is usually necessary to make an initial separate evaluation to develop a baseline before adopting an ongoing monitoring strategy based on changes.

Developing automated monitoring activities for manual controls can be a bit more challenging since the control involves no automation. The opportunity for automated monitoring may be through automated tracking of the performance of the

manual control. This might take the form of an automated log or checklist completed by the persons performing the controls. Although implementing a checklist is quite easy, the solution will probably be unique to that control.

In summary, the suggested strategy is to identify the key controls for monitoring, along with their associated control type(s). Once the control type is understood, monitoring activities can be developed and leveraged. In environments where controls tend to be either inherent or configurable, monitoring activities focus on systems development, change management and configuration management processes. Where the controls are manual or IT-dependent manual, the opportunities to realize significant benefits from automated monitoring may be more limited. Independent of the environment, enterprises will want to leverage existing technology as much as possible to include using solutions/monitoring tools built into systems by the vendors first and only then considering third-party tools.

Identifying Persuasive Electronic Information

Direct information substantiates the effectiveness of controls.

Indirect information, which includes operating statistics and key performance indicators, can also be an effective tool for monitoring.

Indirect information includes operating statistics and key performance indicators. Reports of operating statistics can be modified or combined to show trends and potential failure of controls. In most cases, anomalies in indirect information will require further investigation to determine if they have resulted from a failure of controls.

Since automating controls monitoring is all about information, the first step in the process is determining the suitability of the information relating to the control. A good first step is to consider whether the information meets the COBIT information criteria:

- **Effectiveness**—Describes information that is relevant and pertinent to the monitoring process and delivered in a timely, correct, consistent and usable manner. Direct information is generally more effective than indirect information.
- **Efficiency**—Concerns the provision of information through the optimal (most productive and economical) use of resources
- **Confidentiality**—Concerns the protection of sensitive information from unauthorized disclosure
- **Integrity**—Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations
- **Availability**—Relates to information being available when required by the monitoring process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

- **Compliance**—Deals with meeting the requirements of the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies
- **Reliability**—Relates to the provision of appropriate information for management to operate the enterprise and exercise its fiduciary and governance responsibilities. For monitoring purposes and as discussed in chapter 2, reliable information needs to be accurate, verifiable, and come from an objective source.

Appendix H provides further clarity and application of business information criteria as they relate to automated monitoring.

Developing and Implementing Cost-effective Automated Monitoring Solutions

To develop and implement effective automated monitoring processes, a good understanding of the business processes, business applications, dependencies on automation and integration, and/or IT processes that perform key controls is needed. A good understanding of the automated tools, and the IT processes and requirements required to use those tools, is essential as well. The following is a good practice to follow for these assessments:

- Evaluate the reports and reporting processes already available from the business application or IT general control processes. Most ERP applications, such as SAP and Oracle, have some type of monitoring built into the application instance. For example, Oracle ERP applications have a number of monitoring alerts that can be configured to execute periodically.
- Determine if any of the standard reports from business application or IT general controls operations contain information that may provide reporting for monitoring of key controls.
- Review business requirements with appropriate personnel in the IT department. The IT staff may have existing solutions for special reporting that meet or approximate the requirements for monitoring.
- Evaluate the monitoring tools available. Several good report writing and data analysis tools may already be in use in the enterprise, including, among others:
  - Special-purpose report writing packages that have both report writing and Boolean logic capabilities
  - Database or spreadsheet tools that may meet the enterprise needs, once the appropriate data are accessible
  - Data analysis tools, which are frequently used by audit departments for controls analysis and can be used for operational monitoring of controls

Ensure that the team has the skills and knowledge to design, implement and maintain the analysis tools.

Appendix D provides a more detailed overview of tools and how they might be applied to monitoring of controls.

Planning is critical to achieve the objectives desired from the implementation of the automated monitoring solutions. The plan should include the following activities:

- Requirements gathering
- Data access
- Data preparation
- Data analysis

Variations of this list exist, but the steps within it and the principles used are generally the same.

Requirements Gathering

It is important first to understand the project, define the project's scope and prepare a detailed plan. In the case of a monitoring project, the requirements-gathering step should involve process owners, data owners, system custodians and other process stakeholders.

Data Access

As part of the data access step, management should identify what data are available and how these data can be acquired in a format that can be used for analysis. There are two options for data extraction: accessing the data directly from the source system(s) after system owner approval or receiving data extracts from IT after system owner approval.

The preferred course of action is the first—direct access—especially since this is management monitoring its own controls, not auditors or other third-party entities monitoring management's controls. If it is not feasible to get direct access, a data access request should be submitted to the data owner(s) that details the appropriate data fields to be extracted. The request should specify the method of delivery for the file (i.e., posting on a dedicated server, via e-mail or on compact disc [CD]). Most of the data analysis tools can handle any delimited text file, fixed-length text file or spreadsheet.

Data Preparation

Data preparation readies the extracted data for analysis. The main objective is to perform data quality tests to ensure that data are valid, complete and free of errors. This may also involve making data from different systems suitable for comparative analysis.

Data Analysis

Analysis can involve a simple set of steps or can be a complex combination of steps along with other functionality. Data analysis must be designed to achieve the stated objectives from the project plan.

After the data extracts have been validated (this process can be automated), the enterprise should develop the analysis logic in the chosen data analysis tool. The logic should then be executed and reviewed for errors. At this stage, it may be necessary to troubleshoot testing issues and refine the logic to provide the desired outcome. This step also includes formatting the output for reporting purposes. The output should be reviewed again to ensure that it is providing the correct results. Several iterations of the review and refinement of the logic and output may be necessary. The monitoring process can then be set up to be run on a repeatable basis at the appropriate predetermined sensitivity, range, time and frequency.

Examples of Automated Monitoring

The following examples illustrate different scenarios for monitoring IT controls. Specific tools are referenced in appendix D.

1. Monitoring of configurable system controls—Purchase order approval and data entry accuracy
2. Monitoring system controls—User access and segregation of duties
3. Monitoring system controls—Technology specialist access

Example 1—Purchase Order Approval and Data Entry Accuracy

Scenario
Inaccurate input of purchase orders could lead to financial losses due to incorrect goods or services being purchased. The enterprise should consider taking advantage of various edits or system validations that may be configurable controls in the ERP system for purchase requisitions and purchase orders. The configuration options pertaining to this control may include, but are not limited to, required fields, data validation criteria (e.g., date ranges, allowable currencies, allowable units of measure) and allowable ranges (e.g., reasonable quantities).

Control
An important control for mitigating the risk of inaccurate data associated with the entry of requisitions or purchase orders is to keep constant the system configuration options associated with those transactions, allowing change only when there is a valid business need and after appropriate authorization. In other words, the automated control is that these system configuration options are appropriate, are enforced and remain constant.

Monitoring Activity
An example of an appropriate manual monitoring activity would be a visual inspection of the underlying system configuration or an *ad hoc* system to display that the configuration options for requisitions or purchase orders are set up correctly and are consistent with management's expectations. This assessment would also require the manager to be able to determine that the configuration of the ERP system had not changed by reviewing all changes to the ERP system during the

coverage period (i.e., through manual inspection of a system change log or reviewing a report written by information systems or generated by the ERP system).

Automated Configurable Control Monitoring
The enterprise should consider automating the monitoring of the underlying ERP system configuration. Automated monitoring of these controls would involve automatically monitoring and tracking changes to the system settings described above. Where system settings have not been changed, the automated monitoring routine could automatically record the successful completion of the assessment and the effective operation of information in a database that could be used to report on the associated control.

Automation Requirements
The enterprise could develop an automated routine to compare the configuration settings of the ERP system at various points in time. The routine could be run on a regularly scheduled basis or on demand. Typically, these routines are complex, costly and difficult to develop in-house. In most cases for large complex ERP systems, a third-party tool or external software solution is required. As a result, most enterprises that implement automated monitoring for these types of controls do so using a third-party software package, which also allows the enterprise to implement a continuous monitoring approach.

For these types of controls, a continuous approach would involve using the automated monitoring solution in a continuous monitoring mode—in other words, monitoring the ERP system configuration settings on a daily or more frequent basis and generating an exception-based report whenever configuration options have changed. The advanced capabilities of external software packages allow both continuous and fully integrated monitoring of key automated controls in the ERP system. Additional examples of the types of monitoring capabilities needed to enable a fully integrated approach involve the use of these software packages to enable managers to have immediate access to purchase requisition and purchase-order-related configuration information and potential control issues related to changes to those settings. A fully integrated approach would enable automatic alerts to create an audit trail of all changes to the settings and notify managers when changes have occurred.

Example 2—User Access and Segregation of Duties

Scenario
The user access authorization process is manually intensive, disconnected and lengthy. Access creep is common due to changing roles and responsibilities. The manual process is not integrated across applications and segregation-of-duties considerations are limited and narrowly focused.

Control
Enterprises mitigate these risks through the use of identity management and user access provisioning tools that use workflow tools to enforce access segregation-of-

duties requirements via configured and preventive controls. These preventive controls are established and maintained via a repository of access and segregation-of-duties rules that define the acceptable types of access that can be granted to specific functional roles and the unacceptable combinations of system access that would result in a violation of business rules for the segregation of specific duties.

Monitoring Activity
System owners perform periodic reviews of employee system access based on user access reports generated by IT. The reports are generated separately for each module or system and the process does not facilitate the identification of segregation-of-duties violations across system modules or separate systems.

Automated Monitoring
A workflow-driven authorization process is more efficient and reliable, and preventive access controls reduce risks. Automated monitoring could be set up so that management receives reports of changes to users' access and is alerted to segregation-of-duties violations in real time.

Automation Requirements
Preformatted reports and queries are available from most business systems to enable review of users with access to add, change or delete information through various financial, operational and other business transactions in business systems. However, third-party software packages are often required to provide that information efficiently for more complex systems. Third-party software packages or other custom-developed in-house databases may be required where system access to transactions needs to be monitored across multiple business systems.

Example 3—Technology Specialist Access

Scenario
To prevent unauthorized access to enterprise transactions and data, enterprises typically implement role-based access controls to restrict access to employees that need it to carry out their assigned responsibilities. Technology specialists that support business systems often require access to perform specific business transactions or update business data in the production environment directly. That access is generally granted for a limited time or duration.

Control
A control is needed to give the technology support specialists the required business access to specific capabilities in the production environment for a limited time and to ensure that only authorized actions within the system are carried out. Authorization from appropriate personnel must be obtained prior to allowing the access.

Monitoring Activity
Management must monitor that access is granted to the technology specialist only

as authorized by the appropriate supervisor for a specific business requirement and that the technology specialist is carrying out only those actions necessary to address the specific business support requirements. In accordance with the information security principle of least privilege, only a few user profiles will need to have full access to the production system environment.

Automated Monitoring
For specific user profiles, the enterprise can set up additional security auditing over and above what the system is configured to capture to monitor the access of the technology specialists. Roles can be built granting access to specific roles only to preapproved users. Automated monitoring can be implemented to identify the use of specified employee profiles and the associated transactions or master data changes. If the automated routine flags the use of one of the profiles, a determination can be made whether the appropriate authorization exists. The automated monitoring activity can also be used to report the transactions entered and the data updated so proper review can ensure their agreement with the access request. This makes the employees directly accountable for their actions since there is no uncertainty over who performed which transaction or updated what data.

Automation Requirements
Although predelivered reports and queries are available from most business systems to enable review of users' access, third-party software packages or additional in-house-developed solutions are typically required for more complex systems. Additionally, complex custom-developed in-house databases and reporting capabilities, or alternatively third-party software packages, are usually required to monitor access privileges as well as the detailed transactions used by the employee while granted access to the production environment. Unlike continuous auditing, continuous monitoring is generally performed by business personnel. A formal report on the results should be completed, showing trend information and any unusual variations or control failures.

A case study that integrates the four steps of automated monitoring is provided at the end of this chapter.

Continuous Monitoring

What Is Continuous Monitoring?

Continuous monitoring, as used in this publication, is an IT process or a series of IT processes that operate as an integrated part of a business process for the purpose of detecting control failures on a real-time basis. A continuous monitoring process generally evaluates business transactions with a goal of employing an intelligent process, to detect and report on a timely basis on variations to the expected results of a business control. An example of an IT general control's continuous monitoring process is a program that continuously scans an application system log for unusual or unexpected user access activities.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on a real-time basis. Because continuous monitoring occurs immediately or closely after events in which the key controls are utilized, it enables the enterprise to detect control failures quickly.

Continuous monitoring, which is intended to help ensure that controls are operating as intended, is generally performed by management, as opposed to continuous auditing, which is performed by internal auditors and may have objectives other than those related to controls. However, the scope and objectives of continuous monitoring may be similar to continuous auditing.

Current Management Interest

The concepts of continuous monitoring and continuous auditing have been available, evaluated and discussed for some years. However, the increasing focus on controls and compliance with regulations is causing many enterprise senior managers to take a close look at implementing continuous monitoring processes.

A recent professional survey[9] noted that more than 80 percent of senior finance managers polled are looking to continuous monitoring to help improve the quality of their controls and reduce the cost of compliance. Continuous monitoring is also recognized as a good tool to prevent or deter fraud. Senior managers surveyed indicated that the focus on financial reporting requirements has helped to escalate the interest. However, among the organizations polled, only 25 percent of monitoring testing is automated—leaving plenty of opportunity for growth.

Attributes of a Business or IT Process for Successful Continuous Monitoring

The following attributes will help make the development and implementation of a continuous monitoring project successful:

- **Good sponsorship from the business process owner**—The business process owner needs to understand and agree to the benefits of continuous monitoring of the process. The process owner needs assurance that the monitoring process will not cause failures of the process nor hinder performance.
- **Adequate support from IT management**—A continuous monitoring process is normally an added software module, which needs to run within the IT controlled process. It is prudent for the developer of a continuous monitoring process to follow and work with the IT standard for software development and program change controls.
- **A well-defined scope and objectives for the monitoring project**—It is necessary to determine which controls and processes are in and out of scope, and to define variations to expected results of key controls and a control failure.

[9] McCann, David; "Internal Audit: The Continuous Conundrum," *CFO.com*, September 2009

- **Appropriate data characteristics of the business process or IT process selected for monitoring**—The data need to be reliable. Good supporting documentation that shows expected file and field content must exist.
- **Suitability of direct and indirect information for a continuous monitoring process**—Direct information is the preferred choice to obtain the most persuasive results and best return on the development of a continuous monitoring project.
- **Identification of an appropriate software reporting tool for the selected processing environment**—As previously noted, many modern ERP systems have report writing and control monitoring tools available as part of the implementation of the ERP instance. The ERP modules should be part of a tools selection evaluation. The software audit and reporting tools that have been developed to support internal auditing should also be considered.
- **Project team members knowledgeable in the use of the tool selected**—The team needs to engage appropriate IT developer and/or support personnel who are knowledgeable in the business or IT process as well as the selected tool.

Reporting

Among the key attributes and benefits of continuous monitoring are timely identification and correction of control variations and failures. Identification and correction must be followed by timely reporting as well. Unlike continuous auditing, continuous monitoring is generally performed by business personnel, so a formal report on the results may not be required.

Capability Maturity Model

Automation of control monitoring can range from *ad hoc* queries to repeatable monitoring processes to solutions that integrate monitoring processes into strategic, risk management and performance management processes. Each approach has different challenges and benefits.

Many enterprises continue to view automated monitoring of controls as a discrete activity, separate from mainstream business processes and decision making. They have yet to reach the maturity levels that enable achievement of the maximum benefits for their specific environments.

COBIT provides a process maturity model derived from the Software Engineering Institute's Capability Maturity Model (CMM) to help an enterprise assess its current internal control status and set a target for improvements. An example of a capability maturity model (CMM), describing specific organizational capability maturity levels associated with the implementation and use of automated control monitoring, is included in appendix F. It is not included as a basis for determining what maturity level an enterprise might be from a risk perspective. A maturity level can be assigned to the monitoring process based on the following attributes as they relate to monitoring of controls:

- Awareness and communication
- Policies, plans and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement

Case Study: Theta Company

The Theta Company case study is an example of automated monitoring of controls. It further illustrates how an enterprise can build a monitoring approach over controls at outsourced operations.

I. Scenario

The Theta Company is a mid-sized manufacturing enterprise located in the middle of the United States. Recently, Theta's financial management has outsourced much of its financial transaction process to several providers. Payroll was outsourced to a large payroll processing provider. Purchasing, accounts payable, accounts receivable and portions of general ledger processing were outsourced to a financial accounting service provider named EZ-Accounting Services about six months ago. EZ-Accounting has facilities in the US, but the majority of its processing is performed at centers located throughout Asia. EZ-Accounting has a good reputation and provides accounting transactions services for many companies.

Theta's finance management has always considered the enterprise's accounting transactions services to be well controlled and there is a strong control culture. However, the processes outsourced to EZ-Accounting provided new control and monitoring challenges to Theta. The contract between Theta and EZ-Accounting requires that EZ-Accounting perform control processes compliant with Theta policies and provide Theta with periodic reporting and assurance that the Theta records and processes are adequately controlled. The contract allows for Theta to perform audits at its own expense and includes reimbursement for extra services performed by EZ-Accounting to support the audit.

Theta retained its monitoring process, which is based on indirect information from monthly and quarterly purchasing and cost analyses. Theta found that many of its expenses related to the purchasing of nonmanufacturing materials were higher than expected. Through preliminary reviews, Theta financial management found that receipts for nonmanufacturing materials are possibly not being properly processed and that Theta may be inadvertently charged for purchases made by other EZ-Accounting clients. Management wishes to identify and correct any control deficiencies and to implement additional ongoing monitoring of controls in this process.

II. Designing a Monitoring Program

Theta Company's financial management assigns IT auditor Julie to perform tests of purchases since the inception of the outsourced process to determine if there are problems with the purchasing process at EZ-Accounting and develop an ongoing monitoring program for Theta Company's nonmanufacturing material purchases. This will focus on controls with two objectives:

- The charges to Theta are only for Theta purchases (and not those of other EZ-Accounting clients).
- The charges to Theta for nonmanufacturing materials are supported by receipts.

Since this is a new process and it is outsourced, good documentation for the procurement and payment processing is lacking. Julie has experience with past reviews of the procurement/payment cycle for Theta, prior to outsourcing to EZ-Accounting. From the existing Theta documentation, Julie can gain an understanding of the business requirements and identify key controls in the process.

During interviews with EZ-Accounting personnel, Julie is able to obtain the following:

- Transaction flow documentation for the processing purchase order, invoices and receipts
- EZ-Accounting IT application system documentation that provides file and database documentation, file descriptions and process flowcharts

From Theta she is able to obtain a copy of the warehouse receiving procedures.

To help control the project, Julie creates a project plan, as shown in **figure 17**.

Figure 17—Theta Monitoring Project Plan

Business Case

Theta has recently outsourced the purchasing and payment processing functions, which include a separate process for nonmanufacturing materials. Theta's finance department's analysis shows an unusual trend of increasing nonmanufacturing material expenses. The finance department cannot confirm the reason for the increase, but believes it could be a result of weaknesses in controls at EZ-Accounting. The contract with EZ-Accounting does allow access to records for auditing. However, Theta's business sites are widely distributed across the US and EZ-Accounting processes Theta's transactions in multiple sites in the US and Asia. A full audit to resolve the issues would have a high cost. Theta is processing more than US $5 million a month with EZ-Accounting. Improper accounting of nonmanufacturing materials could have a large impact on Theta's profits and this area has a high potential for fraud.

Opportunity Statement

- Theta's nonmanufacturing material expenditures are currently trending 30 percent greater than expected for current activity, indicating that key controls, such as the requirement for a receipt to support each purchase, may not be adequately performed.
- Theta has no independent assurance that proper accounting and control processes are being followed as required by contract.
- EZ-Accounting is paid based on the number of transactions processed in each area for procurement, accounts payable and general ledger. Payments for services are higher than expected.

Figure 17—Theta Monitoring Project Plan

Goal Statement

Audit a sample of previously processed transactions and also implement an ongoing monitoring process for Theta's nonmanufacturing expenses that leverages existing resources to the greatest extent possible and does not exceed US $12,500 out-of-pocket expenses with the objective to:

1. Confirm receipts of Theta's nonmanufacturing materials expenditures.
2. Confirm that charges for such materials are for Theta's purchases and not for other EZ-Accounting clients.
3. Identify any issues related to EZ-Accounting's compliance with Theta's standards.
4. Remediate the root cause of any discrepancies.
5. Recover losses, as applicable.

Scope

- Nonmanufacturing material expenditures
- Focus on validity of receipts.
- Project does not include any other purchase or payment processes performed by EZ-Accounting for Theta (e.g., manufacturing material, expense reports).

Approach

- Interview appropriate IT staff and review documentation concerning the purchasing program.
- Design sampling approach to select payments since the inception of outsourcing and verify related receipts and appropriateness of charges to Theta.
- Select samples and perform related tests.
- Identify any control weaknesses and needed changes in the procurement process.
- Document an ongoing monitoring process to be run quarterly.
- Implement the ongoing monitoring process with appropriate people.

Time Line

- Validate EZ-Accounting documentation. Week 1
- Design sampling process. Week 2
- Design automated testing process. Week 2
- Obtain files from EZ-Accounting. Week 3
- Perform sample testing. Week 4
- Prepare results. Week 4
- Set up testing process for quarterly monitoring. Week 5
- Report back to Theta management. Week 5

Project Team

- Accounts payable supervisor
- Warehouse operations supervisor
- IT programmer analyst
- Internal auditor

Persons Accountable and Responsible

- The accounting manager is accountable for the overall process and ongoing monitoring.
- The IT manager is responsible for any system changes.

Before Julie can begin, she needs to meet with the management of both Theta and EZ-Accounting. Theta management needs to agree to the plan and provide sponsor-ship. Theta management will contact EZ-Accounting to confirm its support for the project. Julie meets with EZ-Accounting to obtain the files and documentation required.

After Julie obtains the accounts payable receipt and invoice files from EZ-Accounting, she can use a tool such as SAS or PC-based reporting tools, such as ACL or IDEA, to select a sample and analyze the files (see appendix D). Several specialized reports are prepared for the monitoring project.

III. Findings, Root Cause Analysis and Corrective Actions

Julie's team performs a root cause analysis through interviews with the warehouse staff and prepares a cause-and-effect diagram. The team finds that a number of the receipts are improperly coded for Theta sites—in fact the coding is for non-Theta companies. Julie also attempts to match the receipts to invoice records and finds several invoices were paid without proper receipts and charged to Theta. She also finds that the controls performed by Theta accounting personnel are operating effectively.

Julie writes a report of the findings and provides the details to both Theta and EZ-Accounting management. The report details the impact of the control failure. As a result, EZ-Accounting improves its accounts payable matching process and Theta personnel in receiving areas are retrained on how to prepare receipts for nonmanufacturing material. Julie also recommends that the ongoing monitoring process be performed monthly, rather than quarterly, until the number of deviations is minimal. The monitoring process could then revert to a quarterly frequency as originally planned. She also recommends that Theta encourage EZ-Accounting to engage an independent auditor to periodically provide a service-auditor report on controls that could be useful to all of EZ-Accounting's clients as a separate evaluation.

IV. Results

Julie turns over the monitoring process and testing software to the Theta accounting department for its ongoing use. The Theta accounting personnel will continue the monitoring process to help ensure that all payments are supported and EZ-Accounting is in compliance with the Theta standards. Theta senior management receives assurance that payments to EZ-Accounting are properly supported. Theta is also very pleased that they received a refund of previously inappropriate charges from EZ-Accounting, which substantially exceeded the costs of this project.

5. Other Important Considerations

Now that you understand "the fundamentals," drill down deeper.

Look at how this guidance applies to different enterprises and different challenges.

And push further. Examine how different stakeholders of the *same* enterprise view and address these challenges from different perspectives.

Beyond the basic approaches to monitoring IT controls and using IT for monitoring outlined in the previous chapters, special situations sometimes present themselves. These considerations are discussed in this chapter and include the following areas:

- Automating the monitoring process to reduce the cost of compliance
- Recognizing the implications for small-to-medium and large enterprises
- Managing the effects of IT on ongoing monitoring and separate evaluations
- Addressing third-party considerations
- Understanding monitoring implications for auditors

Obviously, not all of these factors will apply to each enterprise seeking a monitoring solution. However, this list highlights a simple truth: setting up a monitoring solution for an enterprise's controls is not a "plug-and-play" endeavor. Rather, careful thought and consideration of these factors in advance of implementing a solution can often save an enterprise time, money and effort in retooling or revising its monitoring implementation.

Automating the Monitoring Process to Reduce the Cost of Compliance

In evaluating the benefits of automated monitoring, an enterprise needs to recognize and consider the upfront and ongoing costs to design, implement and maintain these processes. In general, such costs tend to be more aligned with the nature of other IT costs within an enterprise and can be segmented into areas such as:

- **Application acquisition or development costs**—Costs to acquire or design a monitoring solution using enterprise information or data, develop access to the data, define the business rules and evaluation criteria, build the system-supported processes to review the results (e.g., reports, workflows), and deploy the solution within an IT environment. Potential hidden costs of application development include the automated monitoring procedure's impact on an actual operational system (e.g., potential decrease in system performance).
- **Environment and infrastructure costs**—Costs associated with the technology needed to build and deploy automated monitoring activity solutions. These costs include software, hardware, network and database investments that go beyond what is needed to support the existing IT infrastructure.
- **Maintenance costs**—Costs to find, train and retain resources with skills that can maintain automated monitoring solutions; management overhead costs to maintain these environments; the ongoing costs of maintenance to any developed application and/or maintenance to keep

infrastructure updated with other systems. Maintenance costs are often an overlooked aspect of the total cost of ownership for any IT solution.

Once these costs have been quantified, enterprises can determine if automated monitoring activities can provide a platform for reducing the enterprise's overall cost of compliance and/or increase the value associated with the compliance activities.

The "Four Ares" once again come to mind:

Are we doing the right thing? Are we doing it right? Are we doing it well? Are we reaping the benefits?

It is not monitoring itself; it is monitoring controls effectively and efficiently that helps enterprises reap the benefits.

"Four Ares" as described by John Thorp in his book The Information Paradox, *written jointly with Fujitsu, first published by McGraw Hill in 1998 with a revised edition published in 2003.*

Beyond the risk of being out of compliance with a specific regulation and the opportunity costs associated with noncompliance, ongoing costs associated with compliance efforts that can be reduced through automation include:

- **Control activity costs**—Organization costs, system costs and management costs to execute the day-to-day controls
- **Monitoring costs**—Incremental costs associated with the design, implementation and management of automated solutions for monitoring the system of internal controls
- **Internal validation/assessment costs**—Costs to perform the review and testing of controls required by many regulations to maintain compliance
- **Independent validation/assessment costs**—Costs associated with independent evaluation of controls

By automating the monitoring process, an enterprise may be able to reduce the direct costs of monitoring as well as the costs of internal and independent validations/assessments. Properly implemented, automated monitoring processes and procedures should enable more effective and efficient monitoring of controls by providing access to more comprehensive, timely, frequent, relevant, reliable and cross-system information on the effectiveness of the controls.

Example

An enterprise has implemented various controls within purchasing to ensure that staff adds only authorized vendors to the vendor database. To monitor the effectiveness of the controls over preventing insiders from setting up fraudulent vendor accounts, the enterprise has designed a monitoring activity that compares vendor information to information in its human resource (HR) system. The automated monitoring process extracts relevant data from the HR system (e.g., employee name, address) and compares it to vendor names and addresses in the accounts payable system. The automated routine flags records with identical and/or significantly similar names/addresses for a detailed review.

Manual reviews of large amounts of information to identify identical or similar information are resource-intensive and prone to errors and omissions.

Automation of the monitoring process may reduce the cost of monitoring

compared to manual monitoring activities.

Example

A bank has implemented additional controls for all employee deposit accounts. When new employees are set up, their accounts are flagged and the additional checks and balances are automatically enabled.

To ensure that the controls over identifying all employee accounts are working and an employee flag has not been removed, management has implemented an automated monitoring process to ensure the effectiveness of the account setup controls by running a periodic query that compares HR records with records in the banking application. The query compares names, addresses, telephone numbers, street address, zip codes and other fields for similarities, and routes those that have a certain correlation factor to an independent reviewer for a detailed follow-up.

Automated monitoring activities may appear to be more costly to the enterprise, but they provide a significant improvement in how a control is being monitored and, thus, pay for the investment in the monitoring technology.

Example

Although one might not consider the following an IT example, it provides a good illustration of the broader use of technology for monitoring compliance. IT still has a significant role as it relates to reporting the results and follow-up and closure of violations.

In city government, traffic signals are used to control traffic and reduce the risks of accidents and injury to those traveling on city roads. The traditional monitoring activity for this control has been onsite police officers monitoring drivers' compliance with the traffic signal.

In recent years, more sophisticated photo and motion technologies have been installed to provide more comprehensive reviews of traffic controls. These technologies provide direct information of control compliance and capture documented evidence of noncompliance.

The capital investment in these systems is high, but the automated monitoring solution is continuous and more effective than the manual one. It also increases revenue to the city government and reduces costs related to the appeal process.

In an environment where automated monitoring is effective, *additional* cost efficiencies can be realized during internal or external separate evaluations.

An enterprise may perform a control activity and management may perform

an automated monitoring activity over the control. If the monitoring activity is well designed and executed, it can serve as an ongoing evaluation that the control continues to be effective. As a result, subsequent testing or evaluation of both the underlying control and the monitoring activity is not needed. The assessor/auditor may, at times, actually restrict his/her review to an assessment of the monitoring activity.

Whereas this is true for all monitoring activities, automated monitoring can provide additional cost savings, as the test population for automated monitoring activities, similar to the sample size for automated controls, could be reduced—in some cases, to one.

Automation of the monitoring process can help reduce the overall cost of compliance by reducing one of the major expenses: the cost of independent assessments. Typically, an independent assessor's/auditor's evaluation includes testing both key controls and testing management's monitoring of such key controls. With an effective automated monitoring process in place, an independent assessor/auditor can efficiently gain assurance about key controls by focusing primarily on management's monitoring process.

Recognizing the Implications for Small-to-Medium and Large Enterprises

Not surprisingly, the automation of controls monitoring and its implications tend to differ between small-to-medium enterprises (SMEs) and large enterprises. These differences can be driven by the:

- Organizational structure and system complexities
- Ability and willingness to invest in automated monitoring solutions

The Organizational Structure and System Complexities

Small-to-Medium Enterprises

Due to a flatter organizational structure, SMEs tend to rely more heavily on management oversight and monitoring as a critical part of the internal control system. Managers typically have broad knowledge of an enterprise and a span of control that allows them to build the understanding needed to evaluate controls as a whole. There may even be instances when the person executing the control and the management representative are the same individual.

Most SMEs tend to leverage or augment management's responsibilities with additional evaluation activities over key controls.

Example

A controller in a small chemical processing company with day-to-day knowledge of the plant's purchasing function is aware of customer and vendor issues that may require special purchasing activities. These might include making advance payments as deposits on large purchases (a variance from normal practice) or making emergency purchases from vendors that have not yet been approved by the purchasing function. Although these types of activities could result in control deficiencies in payment approvals or vendor acceptance in a more formalized organizational structure, the controller's closeness is in effect a monitoring activity that minimizes the risk of an adverse impact from these exceptions.

In these environments, monitoring becomes a critical element of the system of internal controls. Just how much management depends on automated monitoring is often affected by how the enterprise uses IT systems to support control activities. Even within SMEs, automated monitoring provides management with the ability to gather more complete, reliable and timely information about a control's effectiveness or failure. Systems can flag potential duplicate payments, create manual journal entry summary listings, track one-time vendor payments or create exception reports to facilitate the monitoring process.

Each SME must define its optimal mix of automated and manual monitoring activities based on its specific circumstances.

Large Enterprises

In large enterprises, automated monitoring is often supported by enterprise resource planning (ERP) applications that can support revenue, expense and financial close business processes and be leveraged by management to evaluate how controls are operating. For example, many controls in ERP applications are configurable and can be monitored as discussed in chapter 4.

ERP applications, business intelligence applications and data warehouse applications provide strong platforms for capturing reliable, timely and relevant information on risks and controls. This information can then be used to monitor controls effectively across business functions, business units and geographies. For example, information about segregation of duties can be extracted and analyzed on a global basis.

The challenges faced by large enterprises usually relate to how to design automated monitoring in a complex business and system environment. These challenges include:

- **Monitoring activities over nonstandard control activities**—Many larger enterprises have variations of business processes and controls that are used to support different businesses or businesses in different

geographies. Defining automated monitoring processes needs to address these complexities for the monitoring process to be effective. For example, a company uses radio frequency identification (RFID) inventory tags to capture inventory. The monitoring tool can periodically track if the assets continue to be within the premises. Exceptions are flagged and resolved in collaboration with the individual to whom the asset is assigned.

- **Collection of control information**—The number of business processes, locations and system environments can increase the complexity of automated monitoring design. Harmonization of control information across systems to identify and react quickly to deficiencies can help remove these inhibitors to effective and efficient automated monitoring.
- **Global nature of operations**—Automated monitoring of controls may require collection of information for different countries and regions, or different currencies and languages. Cross-border data transfer or implementation of standard monitoring processes on a global scale may pose not only technical challenges, but also regulatory issues. For example, information used for monitoring controls over an HR system may include employee personal information. Because personal information is subject to different privacy regulations in each country, cross-border monitoring activities need to consider these differing regulatory requirements.
- **Monitoring across levels of management**—Monitoring of controls can be conducted at various levels of management. This raises specific questions regarding the design of the monitoring process, such as the meaningful aggregation of information or the ease with which senior management can access monitoring results, such as dashboards or workflow reports.

Larger enterprises need to assess automated monitoring as an integrated, enterprisewide process. An enterprise's monitoring needs should be considered during every business process and system development effort. Automated monitoring—especially when integrated across business units, systems and geographical areas—needs to be managed with formal policies, procedures and training.

The pervasive nature of IT general controls makes them a primary target of automated monitoring.

Warning

Many of these solutions focus on application controls and do not consider the impact IT general controls (ITGC) have on the entire system of internal controls. Monitoring solutions for ITGC continue to be piecemeal and generally address only very specific aspects of ITGC, such as access controls. Implementation of automated monitoring solutions for ITGC continue to require the expertise of IT professionals who have a solid understanding of business risk, can identify key related ITGC and are able to implement the monitoring process for these key controls.

The pervasive nature of ITGC may make more complex monitoring solutions pay off where the leveraged benefits and economies of scale and use offset the higher investment and maintenance costs.

Enterprise Ability and Willingness to Invest in Automated Monitoring Solutions

Small-to-Medium Enterprises

SMEs may be more inclined to think they do not have the resources and organizational structures to build an internal control system that can drive efficiencies.

For SMEs that have implemented an internal control system, the challenge is not only to evaluate whether controls are working, but also to ensure that the most cost-effective controls have been implemented and their monitoring has been automated. This inevitably leads to the need to optimize the balance between more formal control activities and oversight/ monitoring activities.

Newer technologies that manage workflow and capture relevant information about controls within business cycles are becoming more affordable.

Example

A SME does not have enough personnel to allow management to implement appropriate segregation of duties for the financial system. As a control, the enterprise has a policy that identifies those transactions that are considered incompatible and are not to be executed by the same individual. All employees are required to read the policy and formally acknowledge their compliance with it on an annual basis.

Management periodically runs a script that identifies if any of the incompatible transactions have been executed by the same individual. The use of the automated monitoring tool has helped assure management that controls are effective and segregation of duties is not being compromised.

Historically, SMEs have not been able to leverage fully existing technology to implement automated monitoring processes. However, the introduction of

newer and more affordable governance, risk and compliance (GRC) software has granted SMEs greater opportunities to implement cost-effective automated monitoring solutions. Many of these solutions can provide monitoring capabilities and utilize workflow to help manage monitoring activities. For example, the price of data analytics tools to monitor application control effectiveness and network scanning tools has become more affordable over the last few years. In addition, many package software applications include monitoring capabilities at little or no additional cost. As new basic data management and workflow technology becomes more user friendly, as tagging technology has wider adoption, and as ERP packages build controls monitoring automation into their software, the complexity and cost of monitoring could be reduced significantly. Users will be able to manage and author their own monitoring data sets requiring less reliance on expensive third-party monitoring tools.

Large Enterprises

Larger enterprises, although they may have more resources and technology available, face similar challenges as SMEs. One such challenge is to project/quantify the return on investment. However, monitoring of controls and operational monitoring can often be leveraged to provide a higher return. For example:

- Information gathered centrally to monitor the control effectiveness of purchasing controls indicates that mobile computing devices are sourced separately and with different terms at each business location. The information is used to centralize purchasing activities and capture volume discounts from the vendor.
- Information gathered during monitoring of system capacity and throughput is leveraged to fulfill the requirement for a data-driven business case during the feasibility phase of the system acquisition process.

Conclusion

While automation of the monitoring process may require significant design, implementation and maintenance efforts, it can benefit management teams and decision makers for enterprises of all sizes by providing insightful information about an enterprise's operations that may not otherwise be available. For example, monitoring key controls related to product quality, development, manufacturing and warranty cost could provide feedback on the respective business processes. Similarly, where there is monitoring of operational information, such as key trends and statistics, there may be an opportunity to use this information or process for monitoring of controls.

Managing the Effects of IT on Ongoing Monitoring and Separate Evaluations

As briefly discussed in chapter 2, one of the attributes that enterprises need to address when establishing a monitoring framework is the frequency of the monitoring activity. Given that most enterprises do not have unlimited resources to devote to monitoring activities, senior management needs to determine the frequency with which a control will be monitored and then plan appropriately.

When determining the frequency with which a control should be monitored, asking and answering a number of questions can be important. These include:

- **Would a control failure have a high risk or impact?** For example, manufacturers often monitor cycle time[10] in production environments, such as car manufacturing. In the case of an automated assembly line, there are controls for ensuring the timely flow of parts and semi-assembled cars from one assembly station to the next assembly station. The failure of a monitoring arrangement over such controls could result in parts shortages, production slowdowns and missed target delivery dates for customers.
- **Are the monitoring frequency and timing aligned with the control frequency?** For example, although account reconciliations are a common business practice, they may not need to be performed daily, especially if the books are closed on only a monthly basis. A monthly monitoring frequency—at the appropriate time of the month—may be most suitable for this scenario. On the other hand, the monitoring process for credit card payment reconciliations will most likely occur more often.
- **Can the monitoring process, in whole or in part, be automated?** Leveraging existing IT to automate parts of a manual monitoring activity enables management to gain more assurance about the effectiveness of controls, often at a lower long-term cost to the enterprise. Management may want to integrate monitoring into daily operations to minimize the impact of a control failure. While not all controls can be easily monitored using automation, management should view IT as a key enabler in monitoring design and implementation and a tool that can render its monitoring efforts a more mature and repeatable process.

As these examples illustrate, while not all controls require the same degree of monitoring, it is crucial that the monitoring arrangements be properly aligned and targeted to deliver the optimum amount of assurance to management.

[10] Cycle time is the period required for one cycle of an operation, or to complete a function, job or task from start to finish (e.g., from ordering, through manufacturing, to delivery). Cycle time is used in differentiating total duration of a process from its theoretical run time.

Ongoing Monitoring, Separate Evaluations or Both?

The monitoring approach should provide the proper balance between ongoing monitoring and separate evaluations, based on potential risk and impact of control failure, time since baseline evaluation, type of information available for monitoring (direct/indirect), frequency of changes, degree of automation of the control, and independence of the evaluator. Management needs to consider whether technology can be leveraged to achieve key goals relative to monitoring. What would be the investment required to do so? When would the enterprise see a return on the investment—and how would this benefit the company's overall control structure? Answering these questions, among others, will help determine how the enterprise will implement ongoing monitoring processes, carry out separate evaluations or perform a combination of both.

Ongoing monitoring represents the classic "always on" type of monitoring seen in many of today's enterprises. This approach is often used when the control is critical to the operations of an enterprise. Ongoing monitoring provides management with the earliest insights into the accuracy, integrity and effectiveness of a given control since monitoring results are often delivered in real time, providing a first alert to the control owners if a problem exists. Ongoing monitoring arrangements are frequently integrated into a system of internal controls and leverage technology to meet the business objectives. Examples of this type of monitoring include reviewing customer returns and complaints, order-to-delivery cycle-time analysis, defect tracking for manufacturing environments, web site availability or application response time for financial services environments, and voltage monitors and temperature controls in nuclear energy production and transmission companies.

Separate evaluations are periodic reviews or revalidations of a selected control. These evaluations are performed on a less frequent basis than those done with ongoing monitoring and are often used to revalidate monitoring results. This periodic check allows management to validate the accuracy and integrity of its ongoing monitoring efforts. Separate evaluations are also applicable where ongoing monitoring arrangements are not in place or not feasible. Examples of separate evaluations may include revalidation of a manual process for report creation, independent periodic inventory validations in warehouse environments, and validation of controls over disbursement authorities on financial systems. Results from this type of monitoring can be used to support decision making on the frequency of the activity (e.g., reduction/increase in the frequency of separate evaluations of a given control or changes in the frequency of ongoing monitoring, reporting on a daily basis instead of an hourly basis and *vice versa*).

Additional Questions and Issues

As noted in chapter 3, it is important to monitor those controls whose success or failure is important to the business. By aligning the design of the monitoring arrangement to the risk profile of a given control set, management can maximize its return on investment by targeting the critical or key controls for monitoring and then choosing whether to implement an ongoing management scheme, separate evaluation or a combination of the two.

One additional aspect for consideration is management's need for information. For monitoring results to be effective for management, they must be timely, relevant and reliable. Without those attributes, the monitoring results may not provide the necessary tactical information to meet management's objectives.

One scenario in which the monitoring process design fails to take the enterprise's overall internal control system into consideration is when monitoring is being executed for a manual key control, while the control itself could be automated with no or little additional investment. In an enterprise where customer refunds require supervisory approval, the manual process may be that the clerk fills out the customer refund form, obtains supervisor approval and refunds the customer. Management periodically reviews the refund log to obtain assurance that supervisory approval was obtained prior to the refund being granted.

The manual review process may be perceived as monotonous and thus performed in a perfunctory manner and the time used to perform the manual review is considerable.

While management may consider automating the monitoring process only, it may instead consider whether similar or better assurance can be achieved by implementing an automated control over the refund process. The clerk can initiate a refund request in the system, which links the request to the customer's original invoice and payment method and electronically delivers the refund request to the supervisor. The system processes only approved refund requests. The monitoring activity consists of management's review of a system-generated refund report.

Automation facilitates ongoing monitoring, which provides more timely information on control effectiveness and reduces the need for more frequent, separate evaluations. Thus the advantages to this approach include the:

- Reduced time to gain information on control effectiveness
- Reduced frequency and cost of separate evaluations
- Potential savings in monitoring costs and personnel effort

In summary, the use of ongoing monitoring vs. separate evaluations is not an "either-or" proposition. Enterprises may have to determine the balance between both types of monitoring schemes to achieve their objectives. It is critical, however, that enterprises align monitoring processes to management's view of the risks, key controls and information requirements for control performance. Failure to properly account for these aspects may put the overall effectiveness of an enterprise's monitoring program at risk and create a false sense of assurance and comfort for management about the state of the control environment.

Addressing Third-party Considerations

Many enterprises see benefits in outsourcing processes to third parties to leverage their capabilities. Some of these relationships are critical and long-lasting, whereas others may merely leverage existing relationships, be project-based, or remain peripheral to the enterprise's overall success. These and many other factors may affect the risk as well as the key controls that are identified as part of the enterprise's vendor portfolio or for each individual third-party relationship. Nevertheless, most vendor relationships start with due diligence procedures during the initiation phase, move through quality assurance processes to ensure continuous value delivery and end with contract termination.

There are, however, significant factors that make control and monitoring activities unique in outsourced situations. For example:

- Whereas the enterprise may be limited in the ability to design and oversee third-party controls and control monitoring activities, management is still ultimately responsible for the achievement of control and business objectives supported by the outsourced process.
- The rights to audit may be unclear.
- The responsibility for internal controls and monitoring of controls is often not well defined.

As a result, it is critical that requirements and responsibilities for controls and monitoring activities be agreed upon during the initial stages of the vendor management life cycle and captured contractually. This publication will not focus on the due diligence process but instead will provide an overview of example-based considerations in situations where third-party relationships already exist. Naturally, these considerations can also be applied to new third-party relationships.

Four main processes are described:

1. Identification of all supplier relationships
2. Supplier relationship management
3. Supplier risk management
4. Supplier performance management

While both controls and monitoring activities within these processes can be manual or automated, the focus is mostly on automated scenarios, as automation of the monitoring process activities can help improve efficiencies and may allow for a more comprehensive monitoring of controls at the service provider. The list of control procedures and related monitoring activities suggested in the following sections is by no means complete and serves merely as suggestion for monitoring of controls when third parties are involved.

1. Identification of all Supplier Relationships

Before an enterprise implements monitoring activities around its third-party relationships, it should consider the contribution of each relationship to the overall achievement of the enterprise's goals and objectives. The more critical the service provider and the higher its risk profile, the more valuable monitoring of key controls may be. Consider the questions listed in **figure 18**.

Figure 18—Questions to Capture and Risk-rank Third-party Relationships
Nature of the relationship: • Is the third party processing critical transactions? • Does the third party have access to confidential data? • Will the third-party processing results impact operations, financial reporting or compliance? • Is the purpose of the relationship to save costs, leverage a third party's experience, improve efficiency, achieve regulatory compliance, or address other factors or a combination? • Is there opportunity for fraud?
Timing: • Is the relationship time-boxed (e.g., annual contract, indefinite contract)? • Is the third party performing processing continuously or periodically?
Extent: • Is the third party on premises or performing its work offsite? • Is the third party embedded in processes or external to the processes? • Is the third party a single or sole source provider? • If the third party was not able to perform its tasks as expected (quality or timing), how would that impact business?

Example Control Practices

COBIT DS2.1—*Identification of all supplier relationships*[11] provides the following control practices:

- Define and regularly review criteria to identify and categorize all supplier relationships according to the supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not recommended.
- Establish and maintain a detailed register of suppliers, including name,

[11] ISACA, *IT Assurance Guide: Using COBIT* and *COBIT Control Practices, 2nd Edition*, 2007, *www.isaca.org*

scope, purpose of the service, expected deliverables, service objectives and key contact details.

Example Monitoring Activity
The supplier database, which is maintained by the purchasing department, is monitored by the legal department to ensure that all third-party relationships, for which they review contracts, are appropriately captured and/or updated, and ranked in the database prior to approving the contract. The answers to the initial questions related to nature, timing and extent of the relationship will help an enterprise determine the risk profile of each third party within the overall third-party portfolio. The higher the risk profile, the greater the need for strong oversight controls and monitoring activities related to those controls. Next step, this input is used to perform a risk assessment related to the processing of data and to determine whether there is data exchange that will increase risk.

2. Supplier Relationship Management

Supplier relationships should be formalized. Formalization in this context is not limited to the existence of valid contracts and/or service level agreements. It also encompasses clearly defined roles and responsibilities, communication processes, and formal incident reporting.

Example Control Practices
COBIT DS2.2—*Supplier relationship management*[12] provides the following control practices (not all are listed):

- Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties.
- Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.

Example Monitoring Activities
Selected contracts are reviewed annually to ensure that the language advised by legal counsel has been incorporated into the documents.

Reports from the vendor database are reviewed periodically to confirm that each key vendor has been assessed for compliance with the agreed-upon service levels at least once in a 12-month period.

3. Supplier Risk Management

Supplier risk management helps identify and mitigate risks related to a supplier's ability to provide effective service delivery in an operationally stable, available, protected and recoverable manner. Third-party related risk

[12] *Ibid*

must be managed throughout the vendor management process and is a function of process-inherent and supplier-specific risks.

Factors to consider when determining the *inherent risk* of the business process to be outsourced include the following:

- **Financial risk**—The risk measured by the impact to the enterprise's financial objectives in case of a service outage, data manipulation, loss of intellectual property, potential fraud and other financial-related incidents. Business processes likely to have financial impact may be hosted e-commerce web sites or payment card processing facilities.
- **Compliance risk**—The risk arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies, procedures or ethical standards and, at times, market pressures
- **Operational risk—**The risk arising from execution of an enterprise's business functions
- **Reputational risk**—The risk associated with negative publicity regarding an enterprise's business practices, whether true or not, that might cause a decline in the customer base, costly litigation or revenue reductions. Business processes likely to have reputational impact are those heavily relying on trust, (e.g., sensitive health information and personal financial information).

Factors to consider when determining *supplier-specific* risks include the following:

- Results of independent assurance reports related to the internal control environment
- Recent control failures
- An enterprise's third-party oversight controls
- The overall ability of the third party to meet the enterprise's needs and level of oversight and staffing

After considering the inherent and control risks, the next step is to determine key controls the enterprise requires as part of outsourcing the business process. At a minimum, an enterprise should expect the same level of security as it requires internally. One effective way to communicate expectations surrounding availability, integrity and confidentiality of information is a data classification and handling policy. This type of policy generally requires information owners to classify information based on a well-defined scheme (e.g., public, internal use only, confidential, strictly confidential) and define specific security requirements for each classification level.

Example Control Procedure

Information is labeled, handled, protected and secured in a manner consistent with the enterprise's data classification categories.

Example Monitoring Activities
A periodic scan is made for data labels on the documents (e.g., network diagrams, policies, guidelines, procedures) within the enterprise's document repository to ensure that all documents are labeled.

A periodic scan is made of the enterprise's hosted web sites for unlabeled information/misclassified information to ensure that document handling procedures are executed in compliance with the document classification criteria.

Example Control Procedure
Key suppliers are required to provide access to internal audit reports or third-party reports upon request.

Example Monitoring Activity
Based on the supplier's risk profile and the enterprise's risk-based audit plan, the supplier's internal audit and/or third-party reports are reviewed.

Supplier Risk Management Associated with Connectivity Architecture

When monitoring controls of a third party, consideration should be given to special connectivity and architecture requirements, including the:

- Benefit from automating the monitoring activities
- Stability of the supplier relationship
- Importance of the supplier to key business operations
- Classification of data being transferred
- Frequency of the data transfer
- Architecture of the connectivity to the third party

An enterprise can define the risk of the connectivity based on the factors of data classification, dependence on the third party and processing by the third party. Based on the risk, a specific type of connectivity architecture should be implemented that includes controls to prevent untrusted entities connecting to the network. Automation of the monitoring process activity could include the discovery of new third-party connections based on automatic security scans. The results of this monitoring activity can enable a security officer to identify rogue connections or connections that do not meet security standards.

Example Control Procedures
Connectivity architecture is commensurate with data classification levels. For example:

- High-risk connections are protected through the use of a high-security architecture using a dual-layer firewall topology and an encrypted tunnel

and prohibition of wireless protocols.
- Medium-risk connections are protected through the use of a medium-risk architecture using a dual-layer firewall topology.
- Low-risk connections are protected through the use of a single-layer firewall topology.

Example Monitoring Activity
An IT scanning tool is used to identify rogue wireless and other connections and determine that architectures in place comply with expected topologies and security measures respective to the third-party risk assessment. Deviations are reported on a timely basis and resolved in a timely manner.

Supplier Risk Management Associated with Regulatory Requirements

Enterprises subject to regulatory requirements need to monitor not only their key controls focused on important regulatory risks, but also similar controls at important suppliers. For example, a hospital may outsource its patient billing and accounting to an outside service organization. Since this processing involves sensitive personal information subject to privacy regulations, the hospital needs assurance that both its controls related to privacy and the controls related to privacy at the outside service organization are functioning effectively.

Management needs to address questions such as:
- Which of its vendors could potentially have a significant effect on its compliance with relevant legal and regulatory requirements?
- What are the most important legal and regulatory risks associated with such vendors?
- What controls are in effect to address these risks?
- How can these controls be monitored?

Using this information, management would then develop a monitoring approach for each vendor having important regulatory risks. This may require special provisions in the vendor contract, including a provision for possibility of regulatory audits of the vendor's activities. In addition, larger enterprises often have a compliance function that can manage this process and may be in a better position to automate monitoring than smaller enterprises.

Example Vendor Controls
Apex Distribution Company uses a vendor to process its product sales billings, some of which are subject to tax depending on the type of product and type of customer. The vendor calculates the monthly tax liability based on billings and prepares a monthly tax statement for Apex. The vendor's billing system calculates the tax with each billing cycle. At the end of the

month a separate automated process independently recalculates the tax, reconciles it to the total of taxes calculated for the billing cycles during the month, and prepares the monthly tax statement. The vendor also has an internal audit function.

Example Monitoring Activity
Apex receives copies of the vendor's internal audit report on the billing system controls and related general computer controls approximately every 12 to 18 months. Apex also receives and reviews a copy of the month-end reconciliation of tax calculated each billing cycle to the recalculated amount at the end of the month. From time to time, Apex independently recalculates the tax due for a billing cycle and compares it to the amount calculated by the vendor in the related month-end reconciliation report.

Supplier Risk Associated with Financial Stability of the Third Party

In performing due diligence on third parties, many enterprises focus on the third party's operations and internal control system. Along with this is the broader issue of supplier risk. Questions should be asked about the third party's financial health, source of funding, audited financial statements, recent news, available third-party financial rating reports, and other factors that could indicate its stability. This should be performed initially before finalizing contract terms and on an ongoing basis thereafter.

Example Control Procedure
The enterprise has a vendor management office that helps to ensure that initial and ongoing due diligence procedures are performed in accordance with company checklists and policies. The checklist and policies require the vetting of the third party's financial stability through the use of standard vetting tools. The information is captured in the third-party database.

Example Monitoring Activity
On a periodic basis, management reviews the third-party database for documents related to the review of the third-party's financial stability and aligns the depth of the reviews to the third-party-related risk assessments.

4. Supplier Performance Management

Supplier performance management encompasses clear reporting between the enterprise and the third party, as well as periodic performance assessments**.**

Example Control Procedure
Individual service providers report monthly on predefined service level agreement metrics via system-generated reports. Examples of tracking metrics might include response time, number of days between when a

problem was reported and the ticket closure date, and call center hold times.

Example Monitoring Activity
Management verifies that monthly reports have been submitted. For those providers that have not submitted reports, management contacts the vendor to determine the reason for not reporting. Management also reviews reports for metrics falling outside the agreed-upon range.

Example Control Procedure
Providers must maintain a user satisfaction rating of three (out of four) over a six-month period to be considered a preferred service provider. All online customers are automatically asked to provide online feedback regarding their satisfaction with the providers.

Example Monitoring Activity
Online customer feedback is analyzed and corrective action is taken after communication with the service provider.

Example Control Procedure
Contracts stipulate that the service provider comply with the enterprise's IT security policies and practices.

Example Monitoring Activity
The enterprise's auditor performs an IT audit to assess compliance with the enterprise's IT security policy.

Understanding Monitoring Implications for Auditors

Once management has established an effective approach for monitoring, these monitoring activities can provide a basis for auditors to establish the effectiveness of controls. Since management presumably has identified key controls that address the most important risks and implemented monitoring activities to ensure control effectiveness, the risk of control failure is most likely low.

When evaluating control effectiveness, it is usually more efficient for internal and external auditors to test the related monitoring activities than the control directly. While the objectives of an external audit are related to the reliability of financial reporting, the objectives of an internal audit can be related to operations, compliance or financial reporting. However, the external and internal auditors can use similar approaches to assess control effectiveness. Auditing of monitoring activities typically focuses on two major questions:

- Are the monitoring activities suitably designed?
- Are the monitoring activities operating effectively?

Assessing the Suitability of Design of Monitoring Activities

Auditors should ask the following types of questions when assessing the design of monitoring activities:

- **Is the design of the monitoring activity aligned to the business objective, risks and related controls it is monitoring?** One example is an automated three-way match of purchase orders, invoices and receiving information as an approval for payment. The business objective is to pay for approved purchases in an efficient manner. A risk in this process is that inappropriate payments will be issued. The control is that a proper three-way match is being made, which directly addresses the identified risk. Management monitors this control by having someone in the treasurer's office "double-check" the support and reperform the three-way match manually for a sample of payments every month. Management also reviews the follow-up on certain items in a three-way-match exception report produced by the system. Management also receives a report of purchasing trends by broad categories of items purchased and reviews this for unusual indications not related to business activities. The auditor would most likely focus his or her review on the "double-check" process, since it uses direct information and focuses directly on the risk of inappropriate payments.
- **Is the information used for monitoring suitable and sufficient?** Continuing the previous example, the "double-check" process uses a file of all paid invoices subject to the three-way match, which the auditor determines is suitable. All payments over a specified amount are tested as well as a sample of those below that amount. The test covers about five percent of the number of payments, but about 45 percent of the monetary value of the payments. The auditor determines this is sufficient to meet the monitoring objectives.
- **Is the balance between separate evaluations and ongoing monitoring appropriate considering the information used for monitoring?** In this example, the three-way match is performed by an IT application, which is very stable. Management performs a separate evaluation whenever major changes are made to the system, but this is infrequent. The auditor concludes that the ongoing monitoring approach is very effective due to the use and sufficiency of direct information and the frequency of separate evaluations is appropriate.
- **Are IT control and other dependencies being appropriately monitored?** In this example, the automated three-way match is dependent on several IT general controls, such as systems change management and access controls. The auditor concludes that management appears to have effective monitoring of these IT general controls and therefore includes this monitoring in the scope of the audit.
- **Is appropriate security in place to protect the integrity of the monitoring arrangements?** Auditors need to ensure that the infrastructure, the application, and the related information are

sufficiently secured to maintain monitoring integrity. In some situations, it may be necessary to utilize a control, such as an electronic "tripwire" within the network or on a server, which notifies the security team and the auditor regarding potential intrusions and unauthorized access attempts. In the above example, the sample of payments is selected each time payments are processed (usually daily). However, the file of items to be "double-checked" is used once each week. Accordingly, to ensure that the integrity of this sample file is maintained, only two employees in the treasurer's department have access to it. Also, the "tripwire" approach is used to report any attempts at unauthorized access to this file. The auditor concludes that the security is appropriate in the circumstances.

The foregoing are illustrative of the thought process an auditor might use when assessing the design of the management process. Having concluded that management's monitoring activities are suitably designed, the auditor would then assess their operating effectiveness.

Assessing the Operating Effectiveness of Monitoring Activities

Auditors should ask the following types of questions when assessing the operating effectiveness of monitoring activities:

- **Is monitoring consistent with business requirements?** In other words, is it occurring in a timely manner? Does it provide for sufficient granularity? Is the information complete or are there gaps where monitoring stopped?
- **Is it repeatable?** Could it be performed by other individuals and still achieve similar results? For ongoing monitoring, would one or more separate evaluations arrive at the same conclusion?
- **Does the monitoring activity provide enough evidence to show whether the control it is monitoring is effective or needs improvement?** Has the use of indirect information provided any indication that there may be a control problem? If so, was further investigation, such as a separate evaluation using direct information, performed to clearly identify the nature of any problem, its cause, and steps needed for correction? Are separate evaluations using direct information performed with sufficient frequency?
- **Based on the auditor's tests of the monitoring activity, do the related controls appear to be operating effectively?** Did the auditor detect any control exceptions that were not detected by the monitoring activity?
- **If exceptions have been identified through the monitoring activity, are appropriate corrective actions being taken or are compensating controls being identified and monitored?** Did corrective action appear to have appropriate address the cause(s) for the exception? Has the control been tested and/or monitoring resumed since corrective action was taken? Have there been steps to investigate whether there were any

related adverse results during the period in which the control was not functioning effectively?

An overall objective for most auditors is to provide management with assurance as to the design and effectiveness of the controls. By focusing on the monitoring process, they can usually obtain this assurance more efficiently while also providing management with assurance that the monitoring process is functioning effectively. Although the objectives and extent of their audit work may differ, both internal and external auditors should strive to utilize the results of management's monitoring activities in their audits to help achieve additional efficiencies and provide additional value to management.

Appendix A. Monitoring and COBIT®, Val IT™ and Risk IT

Introduction

This appendix illustrates the relationship between monitoring and COBIT, Risk IT and Val IT. In addition, examples are provided to help enterprises develop more effective monitoring over IT controls using the COBIT, Risk IT and Val IT frameworks.

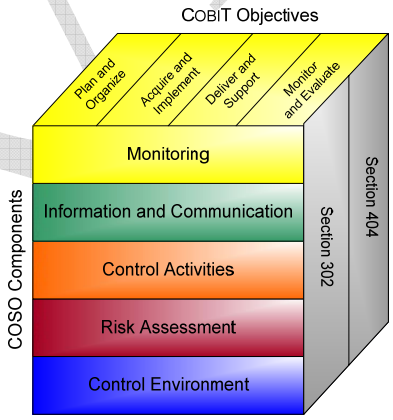
COSO divides internal control into five components. **Figure 19** indicates that all of these need to be in place and integrated to achieve operational, financial reporting and compliance objectives.

COBIT is a comprehensive and generally accepted framework for management of the governance of risk and control of IT. It is widely used by enterprises as a supplement to COSO. It is composed of four domains, 34 IT processes and 210 control objectives. COBIT includes controls that address all aspects of IT governance.

Figure 20 illustrates that COBIT provides detailed guidance similar to COSO, but focused on IT. The five components of COSO—beginning with identifying the control environment and culminating in the monitoring of internal controls—can be visualized as the horizontal layers of a three-dimensional cube, with the COBIT objective domains—from Plan and Organize through Monitor and Evaluate—applying to each individually and in aggregate.

Figure 19—COSO Cube

Figure 20—COBIT/COSO Cube



Monitoring and COBIT

As illustrated in **figure 20**, COBIT consists of the following four domains:

- Plan and Organize (PO)
- Acquire and Implement (AI)

- Deliver and Support (DS)
- Monitor and Evaluate (ME)

Monitoring of IT controls occurs in all four domains to ensure that IT controls continue to operate effectively. Examples of automated monitoring activities or monitoring of IT controls can be found throughout these four domains of COBIT.

This appendix is not prepared to suggest a one-size-fits-all approach nor does it intend to be a complete list from COBIT. Instead, **figure 21** illustrates some examples of monitoring of IT controls; however, each enterprise should assess the nature and extent of automated monitoring activities necessary to support its internal control program on a case-by-case basis based on the results of its risk assessment.

Figure 21—Examples of Monitoring of IT Controls

COBIT IT Process Relevant to Monitoring		Illustrative Examples for Monitoring
#	Description	
Plan and Organize (PO)		
PO1	**Define a strategic IT plan**	IT organizations need to work with business management to ensure that the enterprise portfolio of IT-enabled investments contains programs that are backed up by solid business cases. IT strategic planning is prepared by IT senior management and should be updated annually. An IT steering committee, consisting of senior business executives, should monitor the IT strategic planning process first by reviewing and approving the IT strategic plan to make sure that the IT enterprise strategies are aligned and that the IT strategic plan supports enterprise objectives. In addition, the IT steering committee should monitor the planning process by measuring the effectiveness of the plan. IT management should be accountable for controlling the costs and achieving the planned benefits to provide effective and efficient delivery of the IT components of the program. If there are significant deviations from the strategic plan, including cost, schedule or functionality that might impact the expected business outcomes of the program, the monitoring process would detect and provide an early warning so that remediating action could be taken.
PO5	**Manage the IT investment**	In managing the IT investment, a formal cost and benefit management process should be established in controlling and tracking actual costs to budgets. IT's benefits and contributions to the enterprise should also be identified, documented, reported and monitored. IT management should implement a process to monitor costs on a timely basis. Where there are deviations beyond agreed tolerance, these should be identified in a timely manner and the impact of those deviations on programs should be assessed and reported to management for corrective action. IT management should also implement a process to monitor the benefits from providing and maintaining appropriate IT capabilities. Reports should be reviewed and, if benefits are not being achieved as planned, appropriate action should be defined and taken.
PO9	**Assess and manage IT risks**	An IT risk management process— a senior-management-level responsibility—should be implemented. All identified risks have a nominated owner, and senior business and IT management determine the levels of risk the enterprise will tolerate. IT management develops standard measures for assessing IT risk and defining risk/return ratios. A risk management database is established and the risk management processes are automated. IT risk is assessed

Figure 21—Examples of Monitoring of IT Controls		
COBIT IT Process Relevant to Monitoring		**Illustrative Examples for Monitoring**
#	**Description**	
		and mitigated and results are regularly reported to management. IT management is able to monitor the IT risks and make informed decisions regarding the exposure it is willing to accept. When monitoring an IT risk action plan, enterprises should prioritize and plan the control activities at all levels to implement the risk responses identified as necessary, including execution of the plans and identification of costs and benefits, and report on any deviations to senior management.
PO10	**Manage projects**	A project management office should be established with roles and responsibilities clearly defined and documented. IT projects should be defined with appropriate business and technical objectives and be approved by the IT steering committee. Senior IT and business management should be committed to the effective management of IT projects with defined milestones, schedules, budget and performance measurements. IT management should ensure that a project management process and a methodology are established and communicated. Project communication and escalation processes should be defined, documented and approved. The project risk management process should also be defined and project risks should be identified, documented, assessed and mitigated on a regular basis. IT projects should be monitored by measuring planned against actual milestones, schedules, budget and performance measurements. When monitoring project risks, enterprises should minimize specific risks associated with individual projects through a systematic process of planning, analyzing and reporting on the areas that have the potential to cause the most unwanted change. When monitoring project performance against key project performance scope, schedule, quality, cost and risk criteria, enterprises should identify any major deviations from the plan. Management should monitor remedial action to be in line with the project governance framework, assess the impact of deviations on the project and report results to key stakeholders.
Acquire and Implement (AI)		
AI3	**Acquire and maintain technology infrastructure**	When acquiring and maintaining technology infrastructure, enterprises should implement internal control, security and auditability measures during configuration, integration, and maintenance of hardware and infrastructural software. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. This process should be monitored and evaluated by management to protect IT resources and ensure infrastructure availability and system integrity. The monitoring process should consist of comparing planned against actual measurements; any discrepancies should be reported to management and remediated promptly.
AI5	**Procure IT resources**	The procurement and vendor management processes for IT resources should be documented, approved and implemented. Vendor relationships should be established and maintained over time and the third-party processes should be measured and monitored strategically. IT management should monitor the procurement and contract management processes by evaluating whether they comply with organizational policies and procedures. Any deviations should be reported to management and addressed on a timely basis.
AI6	**Manage changes**	The change management process should be designed and operated effectively for all changes to the IT environment. The process should consist of proper change initiation, documentation, approval and testing. Change management may rely on automated or some manual procedures and controls to ensure that quality is achieved and the change control continues to operate effectively. Change management documentation should be complete and accurate, with changes

Figure 21—Examples of Monitoring of IT Controls		
COBIT IT Process Relevant to Monitoring		**Illustrative Examples for Monitoring**
#	**Description**	
		formally approved, tested and authorized before moving to production. IT change management planning and implementation should be integrated with changes in the business processes to ensure that training, organizational changes and business continuity issues are addressed. A formal process for monitoring the quality and performance of the change management process should be in place to minimize the likelihood of post-production problems.
Deliver and Support (DS)		
DS1	**Define and manage service levels**	The service level agreement (SLA) should be defined, documented and agreed between business and IT based on business requirements. Reports on achievement or deviation of service levels should be provided in a format that is meaningful to the stakeholders. Communication and escalation processes should be defined and agreed upon. All service level management processes should be subject to continuous improvement and service levels reflecting strategic goals of business units should be evaluated against industry norms. SLAs should be monitored and any discrepancies reported to management on a timely basis for corrective action. The monitoring statistics should be analyzed and acted upon to identify negative and positive trends for individual services as well as for overall services. Service levels should be continuously evaluated to ensure alignment of IT and enterprise objectives. Customer satisfaction levels should also be continuously monitored and managed.
DS2	**Manage third-party services**	When managing third-party services, enterprises should establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and performance is continuing to adhere to the contract agreements. The terms of the agreement should be competitive with alternative suppliers and market conditions. The responsibility for managing suppliers and the quality of the services provided should be clearly assigned. Contracts signed with third parties should be monitored at predefined intervals by management and receive independent periodic review. Evidence of compliance with operational, legal and control provisions should be monitored, reported to management and corrective action enforced. Feedback on performance should be provided and used to improve service delivery. Third-party performance measurement provides early detection of potential problems with these providers. Based on results of these measurements, IT management can adjust the process of third-party service acquisition and monitoring.
DS5	**Ensure systems security**	Enterprise IT security policies and procedures should be defined, documented and approved by senior management. Automated processes should be implemented as much as possible to prevent as well as detect any compromises to IT security. Logging functions should be built in to enable early detection and subsequent timely reporting of any exceptional activities that may need to be remediated. IT security should be monitored in a proactive approach in accordance with the current and approved corporate IT security policies and procedures and generally accepted IT security industry standards. IT security should be tested and accredited to ensure that the approved enterprise's information security baseline is maintained.
DS10	**Manage problems**	A formal problem management process should be utilized to properly handle IT problems impacting business users. Agreements should be in place to prioritize problems identified that need to be resolved and acceptable turnaround time determined, based on business requirements. It is important that the root cause of the problems be addressed when problems are identified and a problem resolution database be maintained to reduce the problem resolution time for recurring problems. Throughout the problem resolution process, the problem resolution team should assess the impact of IT problems on the end users involved. In the event that this impact becomes severe, the problem resolution team should escalate critical problems as urgent

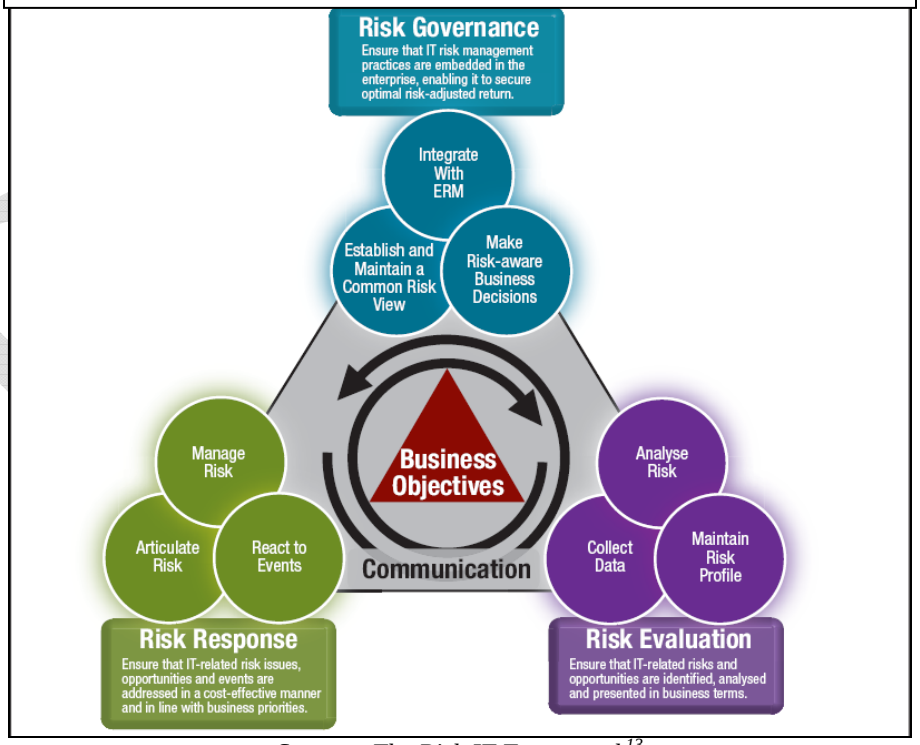
Figure 21—Examples of Monitoring of IT Controls		
COBIT IT Process Relevant to Monitoring		**Illustrative Examples for Monitoring**
#	**Description**	
		changes to an approved board to have the problem addressed as a top priority. Statistics should be maintained to track the number of problems and timeliness of the problem resolution process. IT management should monitor the problem resolution statistics to assess how the problem resolution process can improve over time.
DS13	**Manage operations**	Enterprises should define IT operation processes and standards based on business objectives and industry leading practices. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. These IT operational management processes should be standardized and documented. Effective IT operations management processes help maintain data integrity, and reduce downtime and IT operating costs. Management can monitor the IT operations process and the use of computing resources by reviewing the daily activity reports and comparing them against standardized performance agreements and established service levels. Any deviations from established norms should be addressed and corrected.
Monitor and Evaluate (ME)		
ME1	**Monitor and evaluate IT performance**	Effective IT performance requires an established and approved monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt follow-up of action on performance exceptions. Monitoring is needed to make sure that IT continues to perform effectively according to management policies and procedures. The following are examples for consideration: • Monitoring approach—Establish a monitoring approach to define the scope, methodology and process to be followed for measuring and monitoring the effectiveness of IT controls with a performance management system. • Define and collect data for monitoring—Work with the business to define a set of performance targets and obtain approval from relevant stakeholders. Define benchmarks and establish processes to collect timely and accurate data for comparing actuals against targets. • Monitoring methodology—Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance and fits within the enterprise monitoring system. • Remedial actions—Identify and implement remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through: – Review, negotiation and establishment of management responses – Assignment of responsibility for remediation – Tracking of the results of actions committed • Monitor and evaluate IT performance—Manage the process of monitoring and evaluating IT performance to manage IT cost, benefits, strategy, policies and service levels in accordance with governance requirements.
ME2	**Monitor and evaluate internal control**	Effective IT internal control requires a well-defined monitoring process. This process includes the monitoring and reporting of internal control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations. The following are some examples for consideration: • Monitoring of internal control framework—Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational

Figure 21—Examples of Monitoring of IT Controls		
COBIT IT Process Relevant to Monitoring		**Illustrative Examples for Monitoring**
#	**Description**	
		objectives. • Supervisory review—Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls. • Follow up on indications of failure—Analyze and conduct appropriate follow-up on operating reports or metrics that might identify anomalies indicative of a control failure.
ME3	**Ensure compliance with external requirements**	Effective compliance with external requirements requires the establishment of a monitoring process to ensure compliance with external legal, regulatory and contractual requirements. This process includes identifying compliance requirements, evaluating the existing process, reporting and remediating exceptions, obtaining assurance that the compliance requirements have been met, and integrating IT's compliance reporting with the rest of the enterprise.

Monitoring and Risk IT

As mentioned throughout this publication, the first step for monitoring of internal controls is to identify and prioritize risk. As **figure 22** shows, *The Risk IT Framework* scope is much broader than risk assessment, because it looks at risk governance, risk evaluation and risk response, all which are critical to monitoring. At the same time, the Risk IT framework focuses on meaningful **IT** risks.

Figure 22—Risk IT Framework



Source: *The Risk IT Framework*[13]

[13] ISACA, *The Risk IT Framework*, USA, 2009, *www.isaca.org/riskit*, page 15, figure 6

The Risk Governance (RG) domain ensures that risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. It discusses essential topics, such as risk appetite and tolerance, responsibilities and accountability for IT risk management, awareness and communication, and risk culture to help:

- Establish a common risk view among the "extended" enterprise
- Integrate IT risk management with Enterprise Risk Management
- Help enterprises make risk-aware business decisions

Specific RG process goals are to:

- Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it
- Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level
- Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success

The Risk Evaluation (RE) domain ensures that IT-related risks and opportunities are identified, analyzed and presented in business terms to help:

- IT personnel understand how IT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise
- Business personnel understand how IT-related failures or events can affect key services and processes

Specific RE process goals are to:

- Identify relevant data to enable effective IT-related risk identification, analysis and reporting.
- Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- Maintain an up-to-date and complete inventory of known risks and attributes, IT resources, capabilities and controls as understood in the context of business products, services and processes.

The Risk Response (RR) domain ensures that IT-related issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. It helps:

- Articulate risk analysis results, risk management status, interpret findings, and identify opportunities
- Manage risk through the implementation and periodic inventory of controls, monitoring, risk response and reporting
- React to events by maintaining an incident response plan, monitoring IT risk, initiating risk responses and communicating lessons learned

Specific RR process goals are to ensure that:

- Information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response
- Measures for seizing strategic opportunities and reducing risk to an appropriate level are managed as a portfolio

- Measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective

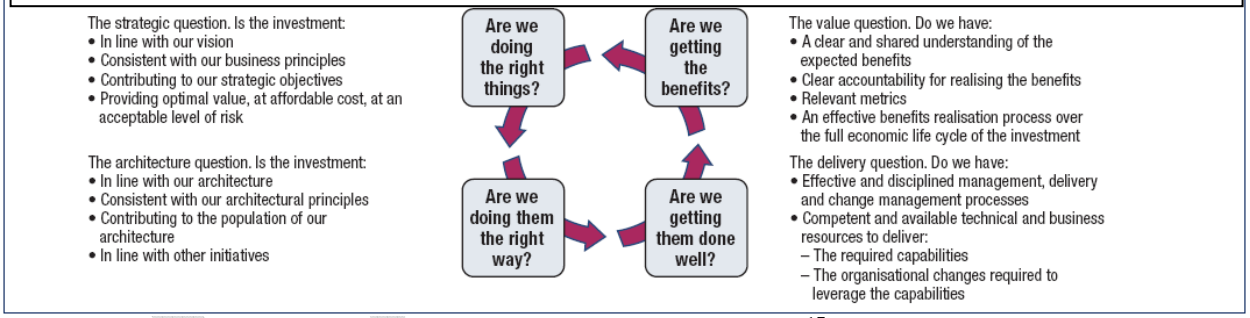
In summary, the Risk IT framework identifies several "essential controls" as well as COBIT control objectives and Val IT key management practices that can be leveraged to identify controls suitable for monitoring. Several appendices in the framework map to known risk management standards and frameworks, such as ISO 31000, ISO 27005 and the COSO Enterprise Risk Management-Integrated Framework.

The Risk IT Practitioner Guide can be used as a solution accelerator, as it provides numerous practical tools that can be used as a solid platform upon which an improved IT risk management practice can be built or an existing IT risk management practice can be improved.

Monitoring and Val IT

The Val IT Framework 2.0 was designed to help enterprises optimize the realization of value from IT-enabled investments. This framework may be particularly useful in step 4 of the monitoring process. Designed to align with and complement COBIT, Val IT integrates a set of practical and proven governance principles, processes and practices and supporting guidelines that help boards, executive management teams and other enterprise leaders optimize the value from IT-related investments. As monitoring of controls is clearly enabled by electronic information and automated controls, it is reasonable to assess IT-enabled monitoring as an IT-enabled program. **Figure 23** introduces the "Four Ares"[14] on which Val IT is based.

Figure 23—"Four Ares"



Source: *The Val IT Framework 2.0*[15]

The Val IT framework consists of three domains: Value Governance (VG), Portfolio Management (PM) and Investment Management (IM).

Of these, IM helps ensure that every IT-enabled investment contributes to optimal value and may be most relevant for enterprises that are considering assessing the value of implementing IT-enabled monitoring activities or implementing an IT-enabled monitoring solution.

[14] The "Four Ares" are described by John Thorp in his book, *The Information Paradox—Realizing the Benefits of Information Technology*, written jointly with Fujitsu, first published in 1998 and revised in 2003, Mc-Graw Hill, Canada.

[15] ISACA, *The Val IT Framework 2.0*, USA, 2008, *www.isaca.org/valit*, page 9, figure 3

The detailed management practices will help IT and business professionals manage the IT monitoring program throughout its life cycle, specifically:

- Develop and evaluate the initial IT monitoring program business case
- Understand the IT monitoring program and implementation options
- Develop the IT monitoring program plan
- Develop full life-cycle costs and benefits
- Develop the detailed IT monitoring business case
- Launch and manage the IT monitoring program
- Update the operational IT portfolio
- Update the IT monitoring business case
- Monitor and report on the IT monitoring program
- Retire the IT monitoring program

Val IT describes three key components of investment management in detail. The first is the business case, which is essential in selecting/investing in the right programs and managing them during their execution. The second is program management, which governs all processes that support execution of the programs. The third is benefits realization—the sets of tasks required to actively manage the realization of program benefits. All three can help the enterprise determine if and how it will invest in an IT-enabled monitoring solution, manage the program throughout its life cycle, ensure that it complements the existing IT-investment portfolio and adds value to the enterprise.

Appendix B. Monitoring and IT Consideration Examples

There are significant efficiencies and benefits that can be realized when IT is leveraged to monitor the operating effectiveness of automated application controls and manual controls that utilize computerized information. Such benefits include increased consistency and coverage, more timely feedback, and opportunities to monitor controls using direct information that otherwise could be monitored using only indirect information.

Controls performed by an IT application generally operate consistently when they exist in a well-controlled IT environment. Effective IT general controls are essential to the effectiveness of most application controls and therefore need to be monitored. Failure to have adequate monitoring of important IT general controls, such as those over programming and data access, could result in placing inappropriate reliance on other controls that depend on IT general controls for their effectiveness.

Development of an approach to monitoring in an IT environment begins with identifying key controls and information that evidences their operation. Such information often can be used for automated tests to determine if the controls are working properly. A well-designed monitoring approach does not involve the monitoring of every business control. It involves identifying which key controls, based on the risk assessment, can be monitored more efficiently and effectively through IT rather than manually.

Case Examples of Application of the IT Considerations

As noted in chapter 2, the six IT considerations are:

1. Key controls that are IT dependent usually are dependent on selected IT general controls.
2. The risk assessment process and the availability of computerized information drive which IT and manual controls will be monitored.
3. Information needed for monitoring may be available only from an IT process.
4. Monitoring of IT controls and automated monitoring often can be leveraged to address multiple monitoring objectives.
5. When key controls are IT dependent, underlying IT general controls need to be monitored.
6. IT facilitates a repetitive, and often a continuous, monitoring process.

Example 1—Complex IT Application

This example illustrates considerations 1, 3, 4 and 6.

IT applications are sometimes referred to as “complex” because the transactions processed within the applications cannot be followed by the use of transaction input and output controls or because they perform calculations or other functions that are not easily checked. For example, the billing and related revenue amounts for the kilowatt hours of electricity consumed by a customer of an electric utility will be calculated based on the hours used, energy usage parameters, time-when-used parameters, the type of customer (residential or business), contractual commitments, and other parameters periodically set in the database.

The key controls in this example might be the systems development and change controls affecting the proper functioning of the calculations, along with the access and integrity controls over the content in the database. The systems development and change controls ensure that the calculations were tested extensively when they were initially implemented and are tested and approved whenever a change is made. Databases generally include various security options relating to the access and integrity of the data input being processed through the databases and relating to the set parameters in the database. For example, many databases can generate checksums that will change if any data are altered. A change in this checksum can be designed to trigger an audit record, an e-mail or similar alert that changes were made to the database information. Monitoring of these IT controls can be an important part of the monitoring process for these complex applications and databases.

Example 2—Three-Way Match

This example illustrates considerations 1, 2, 3, 4 and 5.

An accounts payable system uses an automated three-way purchase-order-receipt-invoice match to approve disbursements and this approval process has been identified as a key control. This control is dependent on a segregation of duties among those individuals authorized to input and change purchase orders, receipts and invoices. This segregation of duties is implemented as an automated process by which employees are authorized online to perform the function by their supervisor and also by an assistant controller. The system produces a weekly report of all changes in the persons authorized to execute sensitive transactions, which includes the names of the persons approving these changes in authorization and highlights any potential incompatible duties. The controller reviews this report to monitor that the persons approving each change are authorized. Semi-annually, a list of all persons authorized to perform sensitive transactions is sent to the relevant supervisor for review and approval, which are then sent to the controller for review.

This approach to monitoring also provides assurance about segregation of duties related to sensitive transactions in other business processes, such as approval of customer orders with nonstandard terms or prices, write-offs of bad debts, and authorizations for making nonstandard journal entries. This illustrates how monitoring an IT control can be leveraged over several business processes and shows the need to monitor an IT control because the information for monitoring is available only from an IT process. Consideration also would be given to the need to monitor related controls such as:

- Controls over changes to the IT application that executes the three-way match
- Controls over changes to the criteria and tolerance levels used for the three-way match
- Review and follow-up of attempts by unauthorized persons to perform sensitive transactions
- Follow-up by the assistant controller and the controller on any unusual changes noted on the weekly and semi-annual access authorization reports

Appendix C. Tools to Manage the Monitoring and Corrective Action Process and How to Implement Monitoring

Figure 24—Monitoring Project Plan Template
Business Case
Opportunity Statement
Goal Statement
Scope
Time Line
Project Team

Supplier, Input, Process, Output and Customer (SIPOC) Diagram

Most business activities are processes and exist to manage some type of business transactions. The SIPOC diagram is a process charting tool commonly used in Six Sigma projects. SIPOC is preferred over common process flows, as it provides a consistent view of any process and allows for limiting the scope of the analysis. All processes are influenced by the sources listed in **figure 25.**

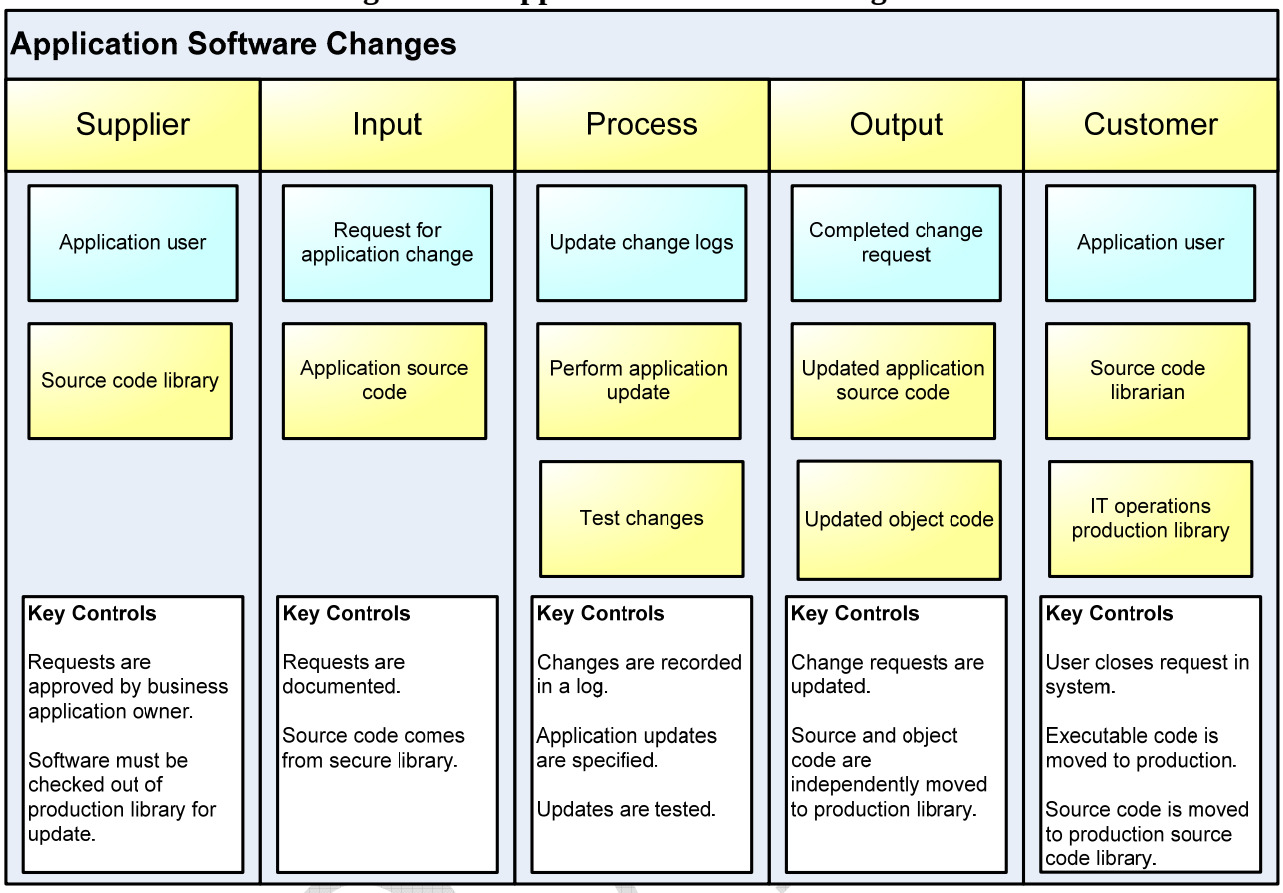
Figure 25—SIPOC Diagram	
Source of Influence on the Transaction	**Description**
Suppliers	Significant internal/external suppliers to the process
Inputs	Significant inputs to the process, such as material, forms, information
Process	Significant steps representing the controls for entire process
Outputs	Significant outputs to internal/external customers
Customers	Significant internal/external customers to the process

The objective is both to illustrate the process for monitoring and identify key controls. Many controls can be classified or identified as having one of the attributes listed in **figure 26.**

Figure 26—Control Attributes	
Attribute	**Description**
Timeliness	Cycle-time requirements for steps in the process
Accuracy	Requirements around how the accuracy of the transaction will be determined and maintained. Control considerations can be input, processing and output controls for each step.
Completeness	How the completeness of the transactions or information is determined and maintained

Figure 27 illustrates an example of a SIPOC for software change control that was developed as part of a monitoring project.

Figure 27—Application Software Changes



Appendix D. Tools for Automating the Monitoring Process

Tools are listed in alphabetical order.

ACL

ACL is primarily a file interrogation tool designed for audit applications that is used for analyzing transactions on a one-time basis. It includes functions such as aging, summarization, stratification and sampling. ACL is able to read ASCII as well as EBCDIC data formats and process large amounts of data. ACL scripts can be set up to perform tests on a repeatable basis; however, user input is required to run the tests when required. ACL can read many formats of data from both ERP and non-ERP systems.

ACL CCM

ACL Continuous Controls Monitoring (CCM) is software that focuses on independently analyzing financial transaction data on an ongoing basis. It identifies areas of control problems and the detail of which transactions failed control tests. It can perform testing of purchase-pay (AP), order-cash (AR), payroll, travel and entertainment (T&E), purchasing cards, and general ledger data while utilizing COSO- and SOX-compliant methodology. ACL CCM has low segregation of duties (SoD) testing capabilities and is not very customizable, as it uses many predetermined tests.

ACL CCM is compatible with any ERP, mainframe system or custom application (using an extract, transform and load [ETL] process), and also has direct-link capability to SAP. It provides an auditable history of compliance tests and follow-up activities. ACL CCM is not, however, a case management system, a dashboard or technology for IT.

Approva Process Insight

Approva's Process Insight software improves visibility into vendor master data, key configuration settings, and exceptional transactions within an enterprise's ERP system. Unusual and inappropriate settings and transactions are proactively flagged. Process Configuration Insight proactively monitors process settings across an enterprise's critical business systems. This continuous monitoring provides visibility into the status of the process configurations and informs the proper stakeholders if unexpected risks are introduced.

IDEA

IDEA is an easy-to-use tool that can quickly and accurately import, join, analyze, sample and extract data from almost any source, including reports printed to a file. IDEA also includes automatic generation of IDEAScripts to aid in the creation of macros to be used on a repeatable basis. IDEAScript is an object-oriented programming language, compatible with Microsoft's Visual Basic and LotusScript.

Infogix Assure®

Infogix Assure is a controls platform software suite that enables a company to quickly develop and deploy independent controls throughout an entire company spanning numerous business processes, applications, databases, ERPs and in-house systems. Controls then automatically capture control source data (in any format) and perform comparisons, calculations, reconciliations, verifications, tracking and other validations in order to determine if the controlled data and processes are performing as expected. Control results are recorded in standardized and custom reports. If needed, control alerts are sent to appropriate personnel and, in some cases, controlled processes are halted to prevent further processing of erroneous or fraudulent transactions. Reports are available to review, test, and audit controls.

Infogix Insight®

Infogix Insight is web-based software that provides a real-time view to automated controls that have been deployed throughout a business. At first glance, users can quickly see which controls (if any) have had exceptions in the past 24 hours. The time frame and dashboard views are easily customized by each user. The user can subsequently click on controls to drill down to specific control runs, control reports and control source data. With a few mouse clicks, one can view controls for a specific business process, controls that pertain to a specific compliance program, or examine what actions have been taken on a given control exception to diagnose and correct the issue. Activities that auditors perform to baseline, walkthrough and test controls are made simple with minimized IT time and support. Controls results trending and analysis can be performed to optimize controls and business process performance.

SAS

SAS is a data analysis tool that can be used on many different platforms, including the mainframe and Windows. It can be applied to voluminous data, non-ASCII data formats or complex calculations. SAS can perform sophisticated statistical techniques and supports multidimensional joining and matching for comparative purposes. It also has the ability to read in complex layouts. SAS programs can be set up to run on a repeatable basis and are able to create some predefined procedures. SAS also provides code and a log for later reference for documentation purposes.

SymSure

SymSure Monitor is a framework used to achieve acceptable levels of risk in an enterprise by monitoring and addressing internal control weaknesses. The solution manages risks and controls from an enterprise level by examining the details of transactions and data files. SymSure has issue management capabilities including assigning exceptions to specific users for action, including users/groups to be alerted for information purposes only, and controlling whether or not the assigned user can close the issue. It also has standardized rules for specific business processes.

Appendix E. IT Key Controls and Related Monitoring Processes

Figure 28—IT Key Controls and Related Monitoring Processes

Risk(s) Addressed	Control		Monitoring Process	Information Used in Monitoring	
	Description	Type		Description	Type
Uncollectible accounts	All accounts receivable credits are approved by management prior to being processed.	Application	Reconcile credits given to credits approved and report exceptions.	• Credit memo (files) • Accounts receivable balances	Direct
Unauthorized access to critical data	Encryption keys are password-protected from unauthorized access.	Application	Employ monitoring software (e.g., Tripwire) and report results.	• File status data	Direct
Unauthorized system changes	All changes are formally approved prior to being moved to production.	IT General	Compare changes to application libraries to approved change requests and report results.	• Application library logs (automated reports of changes to the application library) • Change request log	Direct
Unapproved expenditures	The higher the level of expenditures, the more stringent are the approval requirements.	Application	Review purchase order files to determine if appropriate approval levels were obtained and report results.	• Purchase order files	Indirect
Errors and fraud	User profiles enforce segregation of duties and are granted only upon approval.	Application	Periodically confirm privileges with business management.	• User profiles and related transaction privileges	Direct
Change to or deletion of sensitive files	Set-up of word-writable files requires approval.	IT General	Use scanning software to detect word-writable files.	• File permission settings	Direct
Ability of terminated employees to retain access to corporate system(s)	IT removes employee access within one business day of HR notification.	IT General	Run an extract of the HR system periodically to identify terminated employees for removal of system accounts.	• HR employee data • System/application user reports	Indirect
Failure to protect data from unauthorized access	Password parameters are implemented in compliance with corporate policy.	Application	Inspect or scan system settings against policy and report results.	• Password parameter settings	Direct
Unauthorized system transactions	User are granted system access privileges based on a justified business need.	Application	Review system activity reports for unusual activity and report results.	• Database security log • Operating system security log • Application event log	Indirect
Tendency for problem resolutions to address only symptoms	A root cause analysis is required as part of problem management process.	IT General	Track problem metrics and report to management.	• Problem report (quantity, type, complexity, resolution time, etc.)	Indirect

Appendix F. Automated Control Monitoring Maturity Model

Figure 29—Automated Control Monitoring Maturity Model	
Goal Setting and Measurement	**Tools and Automation**
Level 1 Goals are not clear and no measurement takes place.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage. Monitoring is silo-based.
Level 2 Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired and basic functionality, particularly for packaged solutions, has been implemented. Monitoring is silo-based.
Level 3 Some effectiveness goals and measures are set, but are not communicated. There is a link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application root cause analysis.	A plan has been defined for use and standardization of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan and may not be integrated with one another. Centralized monitoring tools are being introduced. Enterprise monitoring silos are beginning to break down. Monitoring tools to assist with process improvement initiatives are being introduced.
Level 4 Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardized. Continuous improvement is emerging.	Tools are implemented according to a standardized plan, and some have been integrated with other related tools. Tools are being used to automate management of the process and monitor critical activities and controls. Centralized monitoring tools have been introduced. Monitoring is performed by application-specific tools and by centralized tools. Enterprise silos have broken down. A holistic view of risk is available. In the process improvement process, monitoring tools are always used for collection, analysis and assessment of improvements.
Level 5 There is an integrated performance measurement system linking IT performance business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.	Standardized tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions. The business performance and risk management processes have been fully integrated.

Business Value

The organizational maturity model in **figure 30** can be used to drive value throughout the enterprise. Those strategies can be used to move an enterprise from focusing on optimizing internal controls for compliance activities such as Sarbanes-Oxley, to driving tangible business value through organizational realignment to the enterprise's strategies and through business process optimization. As enterprises increasingly apply technology-enabled automated control monitoring capabilities to operations and processes, the value realized is increased through operational and process improvement.

Figure 30—Increased Value from Automating IT Controls

Levels	Strategy	Value	Details
1 to 2	Drive sustainable cost-effective internal controls for compliance	More reliable and efficient controls	More effective and efficient controls enable a sustainable, cost-effective compliance environment.
		More efficient testing process	Automated monitoring can reduce testing efforts. "Self-tests" can reduce sample sizes and automated testing.
2 to 4	Drive operational improvement	More focused internal audit department	Technology-enabled controls are embedded into business processes via roles and responsibilities.
4 to 5	Drive process improvement	Optimized business processes	Technology can drive process optimization via increased efficiencies, improved visibility and real-time decision support.
		Improved management of key processes	Improved visibility into the status of operations, trends and issues supports improved decision support via technology.

Appendix G. Questions a Board or Senior Management Should Ask About Monitoring and IT

Time, resources and funding are common constraints so it is vital to make every new project or initiative count. The board of directors is challenged with ever-increasing regulations with which to comply along with maintenance of day-to-day continued operations. So, where should efforts be increased and how should resources be leveraged?

These are the questions being asked of management across the globe. Applying automated monitoring in the appropriate areas can assist in reducing corporate risk, identifying inefficiencies in controls and gaining comfort at that moment when management is signing off that controls are operating as designed and the financial statements are represented fairly and without misstatement.

Determining where the enterprise can gain the most value and reduce the risk of failure is the optimal goal. The list of questions around IT risk and automated monitoring that board members/audit committee members should consider asking of corporate senior management are shown in **figure 31**.

Figure 31—Questions for Corporate Senior Management

- How does the enterprise ensure that the risk assessment process appropriately addresses IT?
- Is IT risk evaluated and addressed separately from business risk, or is it integrated with the overall risk assessment process?
- How are key application/automated controls used to mitigate identified risks?
- What are the key IT general controls?
- To what extent is monitoring being used to ensure that IT controls are functioning?
- Who is responsible for the monitoring activities over IT controls? The IT department? The compliance department? Internal audit?
- How does the enterprise balance the monitoring activities performed as separate evaluations with ongoing monitoring? What triggers the need for updated separate evaluations?
- To what extent is automation being used to monitor key controls? What automated tools are being used and what do they do?
- For the most important key controls, which are monitored using direct information vs. indirect information?
- What is the extent of continuous controls monitoring being used by the company? What types of controls are being monitored continuously?
- How does the enterprise integrate monitoring activities related to financial reporting, compliance and operations objectives?
- Who is responsible for assessing the risk and controls over third-party vendors on which the enterprise is relying? Is the enterprise monitoring controls at its third-party vendors?

The implementation of the right automated monitoring tools may provide additional efficiencies by performing monitoring over several controls, thereby reducing or eliminating manual efforts and other control-specific tools. A tool added for monitoring and notifying management of server outages and traffic flow optimization may also be able to notify management of event failures requiring immediate responses. **Figure 32** includes additional questions a board member may want to ask of senior management on realizing savings through automating monitoring processes.

Figure 32—Additional Questions Regarding Effects of Monitoring on Resources and Risk
What controls can best be monitored through automated tools? • Transaction processing • IT general controls • Key performance indicators
Where can a reduction in manual efforts be obtained?
Is there cost justification for the automation tool?
Will automating the monitoring process lower the enterprise control risk?

Automated monitoring has the advantage of lowering the risk that an error will slip through the process without identification and remediation since the entire population will be scrutinized at some level. All events would be evaluated to meet specifically defined criteria, at which point the achievement of that criteria would launch a series of notifications and processes to be followed. This eliminates the risk of not selecting a large enough sample to support that the control is operating effectively or using a sample that is not representative of the processes being performed. The cost of automating a control rather than manually testing a significant sample size several times throughout the year would lower with the automation of the process for a control that was found to add value to the enterprise.

There is a misperception that there is a low return on high-cost IT investments. If the investment has not been thoroughly evaluated, that could be true. However, each day brings more compliance requirements accompanied by a reduction in the work force or limited qualified personnel. How can more be accomplished more with less? By automating the processes and limiting the risk.

Appendix H. Relationship Between COBIT Business Information Criteria and Monitoring

As for any business process, the monitoring process must be aligned with business information criteria. The following section provides insight on how business information criteria may affect the monitoring process. The monitoring considerations highlight different approaches to monitoring and how they relate to each criterion.

- **Effectiveness—**Describes information that is relevant and pertinent to the monitoring process as well as delivered in a timely, correct, consistent and usable manner

  Scenario: An office has implemented a physical access control system that requires that employees swipe their access card to gain access to the facility.

  Monitoring Considerations:
  1. Using data from the access control system to determine that the control is working may not be effective, as persons may be able to "tailgate."
  2. Using system logon data and comparing those data to data from the physical access security system may more effectively determine that the control is working, because the comparison would indicate anyone logged onto the system from within the building who did not swipe his/her access card.
  3. Using a camera to monitor that each person swipes his/her access card and does not "tailgate" may be an even more effective monitoring activity**,** but may be inefficient to implement on an ongoing basis.

- **Efficiency—**Concerns the provision of information through the optimal (most productive and economical) use of resources

  Scenario: A hospital has a control in place that requires personnel to track the physical movement of surgical equipment between departments to ensure that usage is properly allocated.

  Monitoring Application:
  1. The hospital collects the physical tracking sheets and reconciles them against usage reports. Manual monitoring of high-value technology assets may not be very efficient, especially in high-pressure, high-risk environments.
  2. The hospital attaches radio frequency devices (RFD) to key surgical equipment. The RFDs are logically assigned to the unique device as well as predefined physical areas. When a surgical device leaves the predefined area, the system alerts the appropriate personnel for follow-up. The automated monitoring process may be more efficient as it frees up resources to focus on patient care as opposed to tracking hospital equipment.

- **Confidentiality—**Concerns the protection of sensitive information from unauthorized disclosure

Scenario: An enterprise has identified key controls within the payroll process and implements automated monitoring activities, which create a file of potential exceptions for follow-up.

Monitoring Application: Since the exception file contains confidential employee information, the enterprise decides to restrict access to the monitoring activity to authorized personnel and distributes the monitoring results directly to the responsible individuals. This practice protects confidentiality of information throughout the monitoring process.

- **Integrity—**Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

  Scenario: The enterprise has chosen to implement a comprehensive monitoring program and has identified the persuasive information necessary to assess each key control's effectiveness. One of the next challenges is to access the information and minimize the possibility of data modification during data extraction, transfer, storage and analysis.

  Monitoring Application:
  1. The project team uses an information request form that can be used to request the necessary information from IT. The information is provided in predefined spreadsheet, database, word processing or text file format. Data integrity may be compromised during extraction, formatting, processing, storage or delivery to the monitoring team.
  2. The project team submitted an information access form and extracts the data directly from the source systems, where applicable. This helps ensure that information used in the monitoring process is less likely to be altered.

- **Availability—**Relates to information being available when required by the monitoring process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

  Scenario: An enterprise implements several monitoring processes with an off-the shelf data analytics tool and assigns one employee as responsible for oversight of the analysis.

  Monitoring Application:
  1. The employee assigned to the monitoring project implements several monitoring solutions on his/her laptop. While on emergency leave, the tool and the scripts may be ready for use; however, the monitoring process cannot be executed as no backup exists and information about the effectiveness of controls is thus not available.
  2. The employee assigned to the monitoring project implements several monitoring solutions on a server. By implementing the solutions on a server, other employees are able to execute the monitoring solutions when the primary person is not available. It is also important to ensure that monitoring processes are well documented to allow for transferability of the monitoring logic and execution to others within the enterprise.

- **Compliance—**Deals with meeting the requirements of the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business

criteria as well as internal policies

Scenario: An enterprise requires employees to comply with an appropriate use of corporate computing resources including Internet usage and collects signed agreements from all employees.

Monitoring Application:

1. In jurisdictions where it is legal to monitor employee e-mails, e-mail traffic as well as Internet endpoints are tracked to ensure that preventive controls are working.
2. In jurisdictions where it is illegal to monitor employee emails, employees may be required to sign "appropriate use of computing resources" agreements, but employee e-mail traffic is not monitored. Monitoring is limited to a management review, ensuring that employees have signed a current "appropriate use of computing resources" form.

- **Reliability—**Relates to the provision of appropriate information for management to operate the enterprise and exercise its fiduciary and governance responsibilities

Scenario: An enterprise has implemented stringent access controls for its ERP application to ensure that only authorized users are granted access to the application.

Monitoring Application:

1. The enterprise has implemented monitoring activities that capture unsuccessful logon attempts in an environment where employees are allowed to share their passwords to allow for job-sharing. While the monitoring activity may function well, the actual control can be so easily circumvented that the information gathered during the monitoring process does not provide reliable information about the effectiveness of internal control.
2. The enterprise has implemented monitoring activities that capture unsuccessful logon attempts in an environment with strong entity-level controls and a robust password policy, which instructs employees not to share passwords. Note that reliability of the information used for monitoring is often affected by other internal control considerations.

References

COSO, *Guidance on Monitoring Internal Control Systems*, AICPA, USA, 2009
COSO, *Internal Control—Integrated Framework*, AICPA, USA, 1992
COSO, *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*, AICPA, USA, 2006
ISACA, COBIT® 4.1, USA, 2007, *www.isaca.org/cobit*
ISACA, *COBIT® Control Practices*, USA, 2007
ISACA, *Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0*, 2008, *www.isaca.org/valit*
ISACA, *IT Assurance Guide Using COBIT®*, USA, 2007
ISACA, *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, USA, 2006
ISACA, *The Risk IT Framework*, 2009, *www.isaca.org/riskit*

Glossary

Accuracy—In monitoring, the degree to which information can reasonably be expected to be free from error and/or the communication of results that reflect reality

Change management—Relative to monitoring, the act of verifying that necessary changes in the design or operation of internal control are made, and made correctly. The goal is to render the internal control system capable of providing reasonable assurance that organizational objectives will be achieved.

Compensating control—An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions. Compensating controls serve to accomplish the objective of another control that did not function properly, thus helping to reduce risk to an acceptable level.

Competence—In monitoring, refers to the evaluator's knowledge of the controls and related processes, including how controls should operate and what constitutes a control deficiency

Continuous auditing—An automated process that allows auditors to monitor business information, controls and system reliability on a real-time basis and to gather selective audit evidence through the computer

Continuous monitoring— An automated mechanism that provides real-time feedback for management to ensure that the systems and controls have been operating as designed and transactions are processed appropriately

Control activities—Activities to implement policies and procedures to help address risks and achieve the objectives of management directives. Control activities occur throughout the enterprise, 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 point in time at which an organization has persuasive information supporting a reasonable conclusion that controls across the entire enterprise or in a given area are designed and implemented to achieve the enterprise's internal control objectives. A control baseline serves as an appropriate starting point for effective control monitoring.

Control environment—Sets the tone of an enterprise 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 organizes and develops its people
- The attention and direction provided by the board of directors

Control objective—A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. Relative to monitoring, control objectives provide specific targets against which to evaluate the effectiveness of internal control. Typically, they are stated in terms that describe the nature of the risk they are designed to help manage or mitigate.

For example, a control objective that all transactions should be properly authorized relates to the risk that improper, unauthorized transactions will occur.

Direct information—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—Individual who is responsible for monitoring internal control at various levels throughout an enterprise. Effective internal control systems include evaluators who have appropriate capabilities, objectivity, authority and resources that enable them to understand the risks that can materially affect the enterprise's objectives, identify the controls that are critical to managing or mitigating those risks, and 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—Information (other than direct information) that is relevant to assessing whether an underlying risk is mitigated and controls are operating. Indirect information does not tell the evaluator explicitly that underlying controls are operating effectively, but it can identify anomalies that are indicative of a potential control failure.

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

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

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

Internal control—Broadly defined as 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:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations

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.

Key controls—When evaluated, provide support for a reasonable conclusion about the entire internal control system's ability to achieve the underlying objectives. They may operate within any or all of COSO's five components.

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

Key performance indicators (KPIs)—Measures that determine how well the process is performing in enabling the goal to be reached.
Scope Note: KPIs are lead indicators of whether a goal will likely be reached, and are good indicators of capabilities, practices and skills. They measure the activity goals, which are the actions the process owner must take to achieve effective process performance.

Key risk indicators (KRIs)—Forward-looking metrics that seek to identify potential problems, thus enabling an enterprise to take timely action, if necessary

Materiality—An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.

Meaningful risks—Those that, in a given time frame, might reasonably have a consequential effect on an organizational objective

Monitoring—In IT, capturing and interpreting information about the use of computers, networks, applications and information. Monitoring, according to COSO's 1992 *Internal Control—Integrated Framework*,[16] is the set of tasks implemented to help ensure that internal control continues to operate effectively.

Monitoring software—A program or set of programs used to oversee computer-based systems and networks for the purpose of tracking usage or identifying, reporting on, and solving problems at the earliest possible stage. Monitoring software is used in a variety of areas ranging from hardware platforms and their components to operating systems, databases, Internet/intranet access and business applications. Typically, different tools are used to monitor individual system components, though the individual monitors might feed information to a higher-level monitor in order to encompass an entire computing environment.[17]

Objectivity—The ability to exercise judgment, express opinions and present recommendations with impartiality. Objectivity is a measure of the factors that might influence any person to report inaccurately or incompletely information necessary for evaluators to reach appropriate conclusions. It includes personal integrity, as well as factors that might motivate even a person with perceived high integrity to misrepresent facts, such as having a vested, personal interest in the outcome of the monitoring procedures.

Ongoing monitoring—Activities that capture and interpret information about the effectiveness of internal control in the ordinary course of operations, including regular management and supervisory activities, comparisons, reconciliations, and other routine actions

[16] COSO, *Internal Control—Integrated Framework*, 1992
[17] Microsoft Computer Dictionary, 5th Edition, Microsoft Press, USA, 2002, *www.microsoft.com/learning/en/us/book.aspx?ID=5582&locale=en-us*

Persuasive 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 sufficiency.

Reasonable assurance—The definition varies depending on the context in which it is being used. The Securities and Exchange Commission (SEC) "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) defines reasonable assurance 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) Statements on Auditing Standards [SAS] No. 1, Section AU 230, 10, defines reasonable assurance for auditors as "a high, but not absolute, level of assurance." For purposes of this guidance, reasonable assurance provided by an effective system of internal control is not absolute, but provides a sound basis for concluding whether the enterprise's related objectives are likely to be met to anyone competent in matters related to internal control.

Relevant information—Relating to controls, 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—Information that is accurate (see accuracy), verifiable (see verifiable) and from an objective source (see objective)

Risk—The combination of the probability of an event and its consequence (ISO/IEC73).[18] Risks can be categorized as:

- Compliance—Risk arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies, procedures, or ethical standards and, at times, market pressures
- Financial—Risk measured by the impact to the enterprise's financial objectives in case of a service outage, data manipulation, loss of intellectual property, potential fraud and other financial-related incidents
- Operational—Risk arising from execution of an enterprise's business functions
- Reputational—Risk associated with negative publicity regarding an enterprise's business practices, whether true or not, that might cause a decline in the customer base, costly litigation or revenue reductions

Risk assessment—A process used to identify and evaluate risks and their potential effects.
Scope Note: Risk assessment includes assessing the critical functions necessary for an enterprise to continue business operations, defining the controls in place to reduce enterprise exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

Every entity faces and must assess a variety of risks from external and internal sources. A precondition for risk assessment is establishing objectives at appropriate levels in the enterprise.

[18] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Guide 73 *Risk management -- Vocabulary -- Guidelines for use in standards*, Switzerland, 2009

Risk assessment is the identification and analysis of risks relevant to realizing objectives, and it serves as a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, flexible mechanisms are needed to identify and address the special risks associated with change.

Self-assessment—Occurs when persons responsible for a particular unit or function determine the effectiveness of controls for their activities. The term is often used to describe assessments made by the personnel who operate the control (i.e., self-review). It can also describe more objective personnel who are not responsible for operating the control. In this guidance, those "other, more objective personnel" would include persons performing peer or supervisory review.

Self-review—In this guidance, refers narrowly to the review of one's own work. It represents the least objective type of "self-assessment."

Separate evaluations—Seek to draw inference about the consistent operation of controls by evaluating controls at a specific point or over a specific period of time. Separate evaluations can make use of all of the techniques used in ongoing monitoring, but they are employed less frequently and are often based on a sample of instances in which the controls operate.

Sufficient information—Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. However, for information to be sufficient, it must first be suitable.

Suitable information—Information that is relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame)

Timely information—Produced and used in a time frame that makes it possible to prevent or detect control deficiencies before they become material to an enterprise

Verifiable—Information that can be established, confirmed or substantiated as true or accurate

ISACA Professional Guidance Publications

Many ISACA publications contain detailed assessment questionnaires and work programs. Please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org* for more information.

Frameworks

- COBIT® 4.1, 2007
- *Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0*, 2008
- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *The Risk IT Framework*, 2009

COBIT-related Publications

- *Aligning COBIT® 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit*, 2008
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing*, 2009
- *COBIT® and Application Controls*, 2009
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, 2007
- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*, 2006
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1*, 2008
- *COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1*, 2007
- *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*, 2006
- *COBIT® Quickstart™, 2nd Edition*, 2007
- *COBIT® Security Baseline™, 2nd Edition*, 2007
- *COBIT® User Guide for Service Managers*, 2009
- *Implementing and Continually Improving IT Governance*, 2009
- *IT Assurance Guide: Using COBIT®*, 2007
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, 2006
- *IT Control Objectives for Basel II*, 2007
- *ITGI Enables ISO/IEC 38500:2008 Adoption*, 2009
- *SharePoint® Deployment and Governance Using COBIT® 4.1: A Practical Approach*, 2010

Risk IT-related Publication

- *The Risk IT Practitioner Guide*, 2009

Val IT-related Publications

- *Enterprise Value: Getting Started With Value Management*, 2008
- *Enterprise Value: Governance of IT Investments, The Business Case*, 2005
- *Val IT™ Mapping: Mapping of Val IT™ to MSP™, PRINCE2™ and ITIL v3®*, 2009
- *Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0*, 2010

Executive and Management Guidance

- *An Executive View of IT Governance*, 2008
- *An Introduction to the Business Model for Information Security*, 2009
- *Board Briefing on IT Governance, 2nd Edition*, 2003
- *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*, 2008
- *Identifying and Aligning Business Goals and IT Goals: Full Research Report*, 2008
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2006
- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Governance—Top Actions for Security Managers*, 2005
- *IT Governance and Process Maturity*, 2008
- IT Governance Domain Practices and Competencies:
  - *Governance of Outsourcing*, 2005
  - *Information Risks: Whose Business Are They?*, 2005
  - *IT Alignment: Who Is in Charge?*, 2005
  - *Measuring and Demonstrating the Value of IT*, 2005
  - *Optimising Value Creation From IT Investments*, 2005
- *IT Governance Roundtable:*
  - *Defining IT Governance*, 2008
  - *IT Staffing Challenges*, 2008
  - *Unlocking Value*, 2009
  - *Value Delivery*, 2008
- *Managing Information Integrity: Security, Control and Audit Issues*, 2004
- *Understanding How Business Goals Drive IT Goals*, 2008
- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2008

Practitioner Guidance

- Audit/Assurance Programs:
  - *Change Management Audit/Assurance Program*, 2009
  - *Generic Application Audit/Assurance Program*, 2009
  - *Identity Management Audit/Assurance Program*, 2009
  - *IT Continuity Planning Audit/Assurance Program*, 2009
  - *Network Perimeter Security Audit/Assurance Program*, 2009
  - *Outsourced IT Environments Audit/Assurance Program*, 2009
  - *Security Incident Management Audit/Assurance Program*, 2009
  - *Systems Development and Project Management Audit/Assurance Program*, 2009
  - *UNIX/LINUX Operating System Security Audit/Assurance Program*, 2009
  - *z/OS Security Audit/Assurance Program*, 2009
- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Information Security Career Progression Survey Results*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Peer-to-peer Networking Security and Control*, 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security, Audit and Control Features Oracle® Database, 3rd Edition*, 2009

- *Security, Audit and Control Features Oracle® E-Business Suite: A Technical and Risk Management Reference Guide, 2nd Edition,* 2006
- *Security, Audit and Control Features PeopleSoft®: A Technical and Risk Management Reference Guide, 2nd Edition,* 2006
- *Security, Audit and Control Features SAP®ERP: A Technical and Risk Management Reference Guide, 3rd Edition,* 2009
- *Security Awareness: Best Practices to Serve Your Enterprise,* 2005
- *Security Critical Issues,* 2005
- *Security Provisioning: Managing Access in Extended Enterprises,* 2002
- *Stepping Through the IS Audit, 2nd Edition,* 2004
- *Stepping Through the InfoSec Program,* 2007
- *Top Business/Technology Survey Results,* 2008