Internal Control — Integrated Framework

Guidance on Monitoring Internal Control Systems

Volume III — Application Techniques

June 2008

Exposure Draft

Public Comment Period
Closes August 15, 2008

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Larry E. Rittenberg
COSO Chair

Mark S. Beasley
American Accounting Association

Charles E. Landes
American Institute of Certified Public Accountants

Edith G. Orenstein
Financial Executives International

Michael P. Cangemi
Financial Executives International

David A. Richards
The Institute of Internal Auditors

Jeffrey Thomson
Institute of Management Accountants

Grant Thornton LLP — Author

Principal Contributors

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

James P. Burton
Partner
Grant Thornton LLP — Denver

J. Russell Gates
President
Dupage Consulting LLC — Chicago

Keith O. Newton
Partner
Grant Thornton LLP — Chicago

Sridhar Ramamoorti
Partner
Grant Thornton LLP — Chicago

Richard L. Wood
Partner
Grant Thornton LLP — Toronto

R. Jay Brietz
Senior Manager
Grant Thornton LLP — Charlotte

Review Team

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

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

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

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

COSO Task Force

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

Douglas J. Anderson
Corporate Auditor
Dow Chemical Company

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

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

Jennifer M. Burns
Partner
Deloitte & Touche LLP

Paul Caban
Assistant Director
U.S. Government Accountability Office

James W. DeLoach
Managing Director
Protiviti

Miles E. Everson
Partner
PricewaterhouseCoopers LLP

Audrey A. Gramling
Associate Professor
Kennesaw State University

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

James E. Newton
Partner
KPMG LLP

John H. Rife
Partner
Ernst & Young LLP

Michael P. Rose
CEO and Senior Partner
GR Consulting LLP

Robert S. Roussey
Professor of Accounting
University of Southern California

Andre Van Hoek
Vice President, Corporate Controller
Celgene Corporation

Observers

Securities and Exchange Commission

Josh K. Jones
SEC Observer
Professional Accounting Fellow

I. Introduction

This volume (Application Techniques or Volume III) of COSO's *Guidance on Monitoring Internal Control Systems* illustrates techniques used by organizations in applying principles outlined in Volume II (the Guidance). The structure of Application Techniques parallels that of the Guidance, providing easy reference between the two volumes.

Chapters II–IV of this volume contain brief examples of various organizations' current monitoring processes, demonstrating the concepts set forth in the corresponding chapters of the Guidance. Chapter V of this volume contains three comprehensive examples of applying the core concepts presented in the Guidance — designing and executing monitoring procedures and assessing and reporting results.

Some users may benefit from first reading the examples in Chapter V in order to gain a more complete understanding of how monitoring might be applied in different situations.

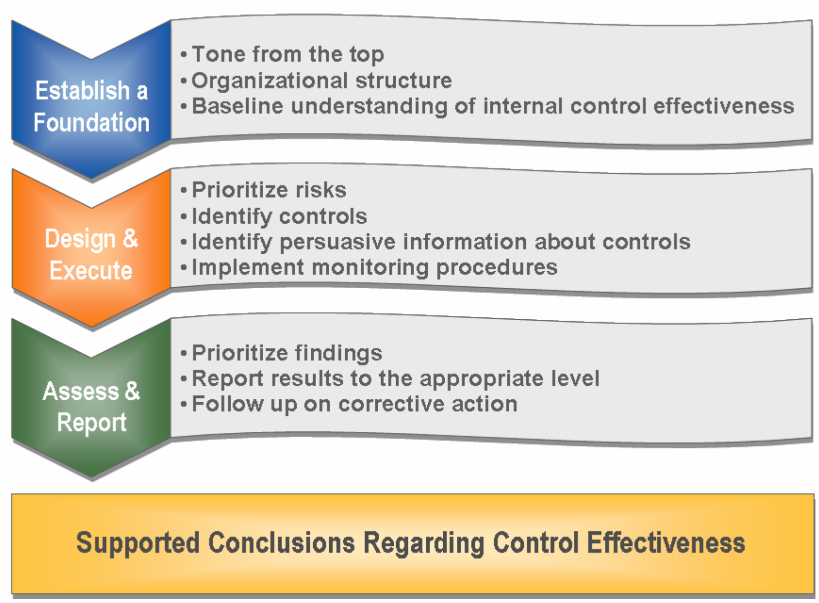
In order to provide further linkage between Volumes II and III, summaries of the Guidance are included in shaded boxes at the beginning of each section in Chapters II–IV. Those passages also provide a foundation for the illustrated techniques. To gain the desired benefit from this material, users should be familiar with the Guidance.

This material is designed to be useful to those seeking to apply internal control monitoring techniques. Proper monitoring of internal control, however, *is not* dependent upon use of the illustrated techniques, nor is their application required for the monitoring component of internal control to be effective. Accordingly, the descriptions and exhibits are presented as examples rather than as preferred methods or "best practices."

While some techniques are best applied in smaller, non-complex organizations, others are more relevant to larger, complex entities — and many can be applied to organizations of all sizes and levels of complexity.

A Model for Monitoring

Guidance Summary: Effective monitoring involves (1) establishing an effective foundation for monitoring, (2) designing and executing monitoring procedures that are prioritized based on risk, and (3) reporting the results, and following up on corrective action where necessary (See Figure 1).


Establish a Foundation
• Tone from the top
• Organizational structure
• Baseline understanding of internal control effectiveness
Design & Execute
• Prioritize risks
• Identify controls
• Identify persuasive information about controls
• Implement monitoring procedures
Assess & Report
• Prioritize findings
• Report results to the appropriate level
• Follow up on corrective action
Supported Conclusions Regarding Control Effectiveness

The Monitoring Process

Figure 1

II. Establishing a Foundation for Monitoring

Guidance Summary: Monitoring is effective when properly planned and supported by the organization. This planning and support form the foundation for monitoring, which includes (1) a tone from the top about the importance of internal control (including monitoring), (2) an organizational structure that considers the roles of management and the board in regard to monitoring, and the use of evaluators with appropriate capabilities and objectivity, and (3) a baseline understanding of internal control effectiveness.

Tone from the Top

Guidance Summary: As with every internal control component, the ways in which management and the board express their beliefs about the importance of monitoring have a direct impact on its effectiveness. Management's tone influences how employees conduct and react to monitoring. Likewise, the board's tone influences how management conducts and reacts to monitoring. The following examples highlight ways in which various organizations have implemented an effective tone from the top.

Many of these examples are broad, covering the tone from the top regarding the importance of *all* internal control, including monitoring. Others demonstrate how management effectively and consistently communicates its expectations regarding risk and the importance of monitoring in providing assurance that meaningful risks are properly managed or mitigated.

Consistent development and communication of expectations regarding internal control, including monitoring

Example 1: A large professional services organization maintains what it calls a "COSO Usage Document." This document, updated annually, identifies how the organization achieves the principles and attributes of each of the five COSO components. The contents of the COSO Usage Document are validated by the global leadership responsible for processes across the enterprise (i.e., Finance, HR, CIO, Legal, Operations). In addition to serving as a key design document which helps management and the auditors understand the strength of their design, the COSO Usage Document also serves as evidence of the organization's integrated control structure. Readers receive a clear message from the top of the organization that internal controls, including monitoring, are an important part of the success of their business. See Appendix A for excerpts from this COSO Usage Document.

Use of a formal risk committee to develop and communicate monitoring expectations

Example 2: A large power generation company has established a Risk Oversight Committee (ROC) to focus on risk management and oversight of the company's operations. The ROC includes members of senior management and is an active part of the monitoring structure. The ROC sets the proper tone from the top by:

- Establishing Risk Policies and the organization's Business Risk Profile,
- Monitoring compliance with the Risk Policies, and
- Ensuring that operations are managed within the boundaries set in the organization's Business Risk Profile.

Internal audit policy that encourages self-assessment and self-reporting of potential control problems

Example 3: The internal audit department of a financial services organization has implemented a rewards system that encourages departments to monitor the effectiveness of their internal control systems and self-report possible control deficiencies. This encouragement comes in the form of an internal audit policy that gives departments credit in the internal audit grading system for deficiencies that are self-reported. Deficiencies that are identified through an internal audit examination, rather than through a department's monitoring efforts, are counted against the score.

This credit for self-reporting does not preclude internal audit from reporting specific deficiencies to management or the board when such reporting is warranted, but it does positively affect the grading system, which can affect departmental compensation and benefits, thus increasing the likelihood that control deficiencies will be identified and corrected before they can become material to the organization.

Organizational Structure

Clearly articulated roles and responsibilities through the establishment of preparer/reviewer standards for key journal entries

Example 4: In relation to financial reporting risks, an international consumer products company developed a detailed description of the roles and responsibilities of journal-entry preparers, detail reviewers and secondary reviewers. The organization then developed a matrix of key journal entries (i.e., those with direct financial statement impact, primarily for the major functional corporate areas including tax, accounting, treasury, legal, etc.), and compared that matrix to the policy.

Through this analysis the organization determined that, in several complex areas, it did not have appropriate levels of journal-entry review. The organization developed a plan for each identified deficiency — mandating the formal sign-off by the preparer, detail reviewer and secondary reviewer for each key journal entry.

Independent personnel periodically select a sample of journal entries and evaluate compliance with the policy. The audit committee receives a report on the test results and reviews the key journal entry matrix on an annual basis.

Use of a formal risk committee to develop and communicate expectations

Example 5: Senior management at a provider of Internet-based securities brokerage and financial services has established a formal Corporate Risk Committee (CRC) tasked with facilitating the completion of an enterprise risk management program. One of this committee's mandates is to determine and communicate how the organization will monitor controls over the risks identified in its annual Corporate Risk Assessment process. As a result, management has a "road map" in which financial and operational controls in the business are linked to the risks identified during the annual risk assessment.

Creation of a Risk Control function to facilitate both the development of controls and the monitoring of those controls

Example 6: An energy company created a new Risk Control function to address risks related to its complex energy trading operations. The addition of this function to the organization's structure enables the company to better monitor the internal control system's ability to address some of the organization's highest operational, financial reporting and compliance-related risks. It also sends a message throughout the organization that management is committed to monitoring the effectiveness of internal control.

Smaller organizations in similar situations (i.e., those in regulated industries, with unique, highly complex, highly material risks) may not need to establish a separate risk control function within the organizational structure. They might, instead, assign specific management or other independent personnel to (1) obtain and maintain appropriate skills and training, and (2) perform ongoing monitoring and periodic separate evaluations in those high-risk areas. If deemed necessary, smaller organizations could also engage qualified external professionals to help monitor the internal control system's ability to manage or mitigate these unique risks.

Clear assignment of oversight responsibilities

Example 7: A small software company has an organizational chart for its corporate accounting department that is updated as new employees are added. Responsibility for overseeing financial reporting processes and monitoring controls in key areas (e.g., Financial Reporting, Payroll, Human Resources, Payables and Billings) are assigned to appropriate personnel. The Audit Committee conducts an annual review of the organizational chart and oversight responsibilities.

Role of Management and the Board

Guidance Summary: Management has the primary responsibility for implementing effective internal control, including monitoring. As it relates to monitoring, the board is responsible for determining whether management has implemented effective monitoring procedures where necessary. It makes this assessment by (1) understanding the risks the organization faces, and (2) gaining an understanding of how senior management manages or mitigates those risks that are meaningful to the organization's objectives.

The board also monitors — often through the use of a competent and objective internal audit function — those controls that senior management cannot objectively monitor, such as controls that address the risk of senior-management override.

Audit committee's use of internal audit to address certain risks

Example 8: In order to determine that management has implemented effective monitoring procedures over certain identified risks, the audit committee of a small, global manufacturing company has directed internal audit to perform specific annual reviews. One area of specific concern is manual journal entries, with a particular focus on potential management override activities. Internal audit's review includes basic information such as the number, dollar amount, preparer, business unit, and timing relative to month- and quarter-end. This analysis also includes more in-depth information such as:

- Reasonableness of significant entries (e.g., manual entries in traditionally automated accounts such as inventory),
- Review of the appropriateness of the individual performing the journal entry (e.g., senior executives or unauthorized personnel),
- Review of the frequency of journal entries, particularly relevant to management authorization levels (e.g., to identify potential statistically anomalous entries using Benford's Law[1]),
- Identification of journal entries without descriptions,

[1] Benford's Law, also knows as the "first-digit law," is named for the late physicist Dr. Frank Benford. Building on a theory first proposed by the astronomer Simon Newcomb in 1881, Dr. Benford proved that in lists of numbers, leading digits typically are distributed in a specific, non-uniform way. According to Benford's law, the first digit is 1 approximately 30 percent of the time, and larger numbers occur as the leading digit with less and less frequency as they grow in magnitude. Benford's Law is frequently used to search for instances of error or fraud.

Potentially fraudulent entries. The organization created a profile of potential fraudulent entries from management override frauds known to have been perpetuated at other companies. Internal audit statistically compares the manual journal entries against this profile.

Use of self-assessments to instill monitoring responsibilities throughout the management structure

Example 9: A provider of Internet-based securities brokerage and financial services has instituted a formal Internal Control Assessment Program (ICAP). This program requires business unit owners, on a quarterly basis, to perform a control self-assessment and certify the effectiveness of certain controls for which they are responsible. Management clearly communicates its expectations regarding the accuracy of the ICAP certifications and holds managers accountable if they improperly certify their internal controls.

Management recognizes that self-assessment, while not completely objective, is an effective first line of defense against internal control failure. As a result, management is able to focus more-objective monitoring where the level of risk warrants. Furthermore, Internal Audit helps compensate for the lack of objectivity in the control self-assessments by performing independent monitoring procedures on a periodic basis and comparing their results to the self-assessments.

Internal Audit modifies its annual audit program, which includes both ongoing monitoring and separate evaluations, based on the results of:

- The organization's Annual Enterprise-wide Risk Assessment,
- The results of the business unit owners' Internal Control Assessment Program (ICAP),
- Internal Audit's own risk assessment process.

Use of internal audit to assist in risk assessment and monitoring activities

Example 10: An international manufacturer has an internal audit function that is both functionally and administratively independent from the CFO, CEO, and business unit leaders. The internal audit department aligns its annual objectives with the enterprise-wide strategic objectives. As a result, the focus of the annual audit plan is consistent with the corporate strategic objectives at the corporate and business unit level. Furthermore, audit budgets include time allocated for additional requested reviews and projects that can be initiated at the request of any executive within the organization, and executed upon approval of the corporate audit committee.

Board of directors' oversight adjusted based on risk

Example 11: The board at a medium-sized manufacturing company has standing responsibilities that ensure that they have visibility to key risk areas. For example, they recently determined that contract compliance was a high-risk area that warranted board oversight. Accordingly, they implemented a requirement that the board review and approve any sales contracts over $50M or greater than five years in duration, and any corporate contracts that vary from standard terms.

Open lines of internal and external communication

Example 12: A large governmental agency has multiple stakeholders. With respect to fraud, waste, and abuse, this organization's inspector general is authorized to report on matters identified from its 1-800 hotline for anonymous callers, e-mail box, FraudNET,[2] etc. Further, the general counsel's office has a forensic audit team who is called in when investigations are warranted.

Characteristics of Evaluators

Guidance Summary: Effective monitoring is conducted by evaluators who are appropriately **competent**[3] and **objective** in the given circumstances. Competence refers to the evaluator's knowledge of the controls and related processes, including how controls should operate and what constitutes a control deficiency. The evaluator's objectivity refers to the extent to which he or she can be expected to perform an evaluation with no concern about possible personal consequences and no vested interest in manipulating the information for personal benefit or self-preservation.

Lessons learned from the correction of a difficult monitoring and oversight problem

Example 13: Executive management at a medium-sized manufacturing company has modified its monitoring to include more ongoing monitoring of internal control over financial reporting at the corporate level and reduce the frequency and scope of separate evaluations at plant locations. This shift resulted from corrective action taken after the organization identified the following internal control problems that had a direct impact on its ability to monitor its internal control system effectively. The organization determined that it:

- Lacked appropriate internal ownership of risks and controls related to financial reporting, and
- Had an insufficient number of competent personnel throughout the organization who could effectively monitor controls that address financial reporting-related risks.

Senior management, through ongoing monitoring at lower levels, did not receive enough direct information regarding the operation of key controls. As result, it was forced to conduct year-end separate evaluations of internal control that were not as efficient as they could have been if more-effective ongoing monitoring had been present.

[2] FraudNET is a communication vehicle through which the public can report allegations of fraud, waste, abuse, or mismanagement of U.S. federal funds.

[3] Bold items are defined in the Glossary to Volume II.

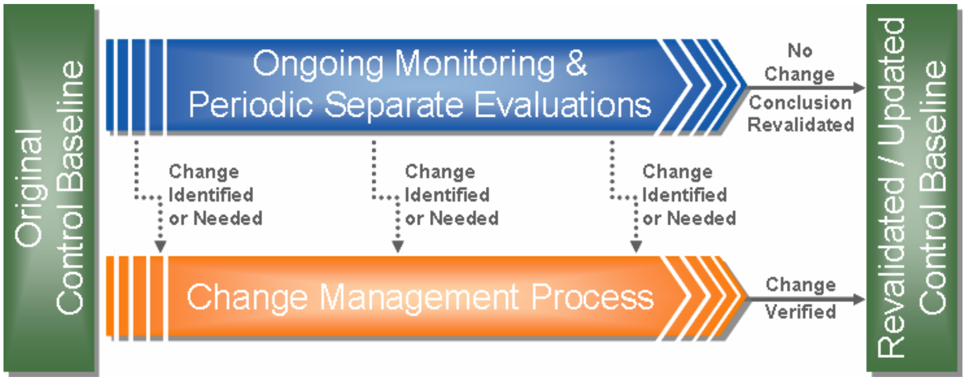
Driven by the audit committee’s desire to see immediate improvement in the completeness, accuracy and integrity of financial information and internal control, the organization made a number of changes, including extensive personnel changes, and new external advisors. However, the company did not realize an immediate improvement in the results, as numerous accounting errors and significant internal control deficiencies continued to surface. The organization had taken steps to correct the personnel issues, but some procedural issues remained to be addressed.

For some of the exceptions, up to five different reviewers had signed off on reconciliations that contained errors. Further analysis of the continuing errors revealed that historical knowledge of certain accounting matters and reconciling items was lost as a result of the turnover in personnel and a lack of previously developed supporting documentation. In addition, the new personnel suffered from a lack of procedural documentation or training for their new jobs, which affected their ability to operate effectively.

The organization corrected these monitoring problems by eliminating unnecessary monitoring redundancies, formally assigning monitoring responsibilities over accounts and controls, documenting the monitoring processes, and properly training personnel. With these adjustments in place, the momentum shifted considerably. The company began to identify and address exceptions and accounting issues in a more timely, accurate and efficient manner. In addition, the increased competence and objectivity of the new personnel allowed the organization to identify improvements in the monitoring information supplied to senior management throughout the year. As a result senior management has been able to conduct more ongoing monitoring at the corporate level, and reduce the frequency and scope of separate evaluations in the plant locations.

Baseline of Effective Internal Control

Guidance Summary: Monitoring starts with a supported understanding of the internal control system's design and of whether controls have been implemented to accomplish the organization's internal control objectives. As management gains experience with monitoring, its baseline understanding will expand based on the results of monitoring. If an organization does not already have such a baseline understanding in an area with meaningful risks, it will need to perform an initial, and perhaps extensive, evaluation of the design of internal control and determine whether appropriate controls have been implemented. An established baseline understanding of internal control effectiveness provides an appropriate starting point for more-effective and more-efficient monitoring that focuses on changes either in the environment or in the internal control system (sees Figure 2).


Original Control Baseline
Ongoing Monitoring & Periodic Separate Evaluations
No Change Conclusion Revalidated
Change Identified or Needed
Change Identified or Needed
Change Identified or Needed
Change Management Process
Change Verified
Revalidated / Updated Control Baseline

Monitoring for Change Continuum

Figure 2

Effective use of a control baseline

Example 14: A beverage manufacturer and distributor alters the type, timing and extent of its internal control monitoring based on the results of its risk assessment process (see Example 17:). In areas of meaningful risk the company first "benchmarks" the key internal controls, meaning they conduct a thorough review of the design and operating effectiveness of the controls in order to establish a baseline of effective control. With the risks prioritized and the benchmark established, management (with the assistance of internal audit) identifies controls that can be monitored for a reasonable period of time through more-efficient monitoring techniques such as using indirect information or self-assessments coupled with supervisor review. On an interval that is commensurate with the level of risk, internal audit performs periodic separate evaluations of key controls, thus reconfirming the benchmark and the effectiveness of the ongoing monitoring procedures.

Modification to monitoring as a result of an identified change in the environment

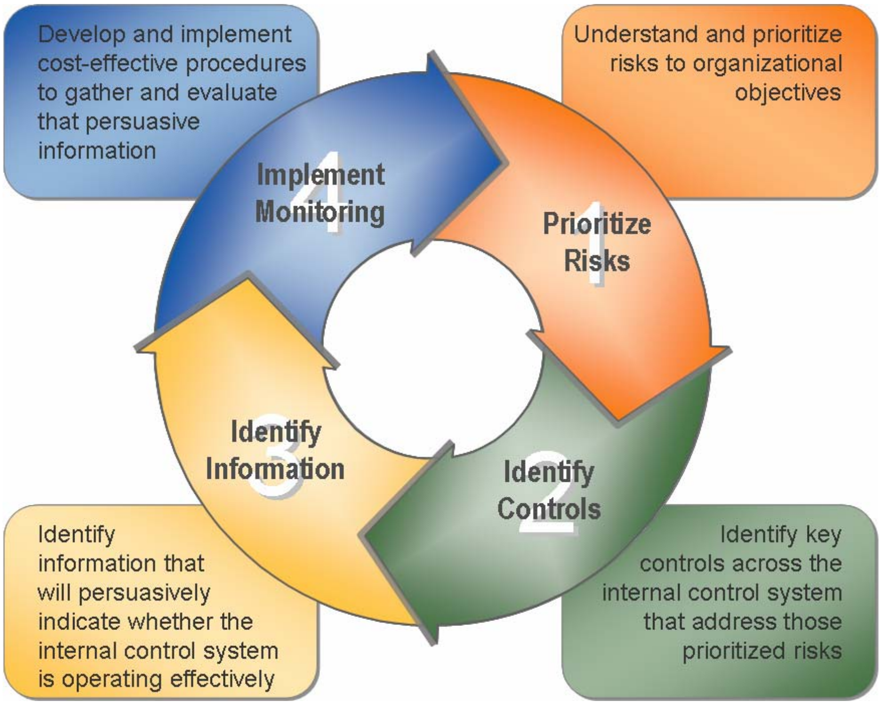
Example 15: A small semiconductor research and development organization recognizes that many of its financial statement risks reside with the selection and application of accounting estimates. As a result, it conducted an initial risk assessment that identified the following related risks:

- Calculation of allowances for uncollectible accounts, inventory obsolescence, and deferred tax assets,
- Methodology for updating standard costs,
- Review of cost provisions regarding its government contract and the methodologies used to identify unallowable costs and allocations,
- Procedures to test for possible impairment of assets,
- Update of the annual evaluation of goodwill for possible additional impairment analysis, and
- Search for possible loss contingencies related to litigation, environmental remediation, or possible product warranty liabilities.

With the initial risk assessment completed, the organization can effect efficient updates through periodic discussion of factors that prompt reprioritization of these risks and evaluation of any new risks. For example, the company closed a major plant during one fiscal year. As a result of this identified change, management considered the related risks and determined to evaluate controls associated with accounting for discontinued operations, including the process for capturing all costs associated with the closed facility. Identifying the change in the environment led to an assessment of the related risk and to at least a temporary modification of the internal control monitoring procedures.

III. Designing and Executing Monitoring Procedures

Guidance Summary: The core of effective and efficient monitoring lies in designing and executing monitoring procedures that evaluate important controls over meaningful risks to the organization's objectives. An overall model of monitoring is shown in Figure 3 below that may help in designing and implementing the monitoring component. The model reiterates the importance of understanding risks and the relationship of controls to risks as both a fundamental part of the COSO Framework, and an integral part of monitoring as well.


Develop and implement cost-effective procedures to gather and evaluate that persuasive information
Understand and prioritize risks to organizational objectives
4 Implement Monitoring
1 Prioritize Risks
3 Identify Information
2 Identify Controls
Identify information that will persuasively indicate whether the internal control system is operating effectively
Identify key controls across the internal control system that address those prioritized risks

Logical Monitoring Design Progression

Figure 3

Understand and Prioritize Risks

Prioritize Risks

> Guidance Summary: Designing effective monitoring begins with understanding and prioritizing the risks to achieving important organizational objectives. Prioritizing risks helps identify which risks are meaningful enough to subject to control monitoring.

Adjustment of type, timing and extent of monitoring based on the results of risk assessment

Example 16: Senior management of a beverage manufacturer and distributor focuses the organization's monitoring efforts by location and by risk priority. Risk considerations include areas:

- That are material or complex,
- Where systems or processes have changed significantly,
- Where errors or irregularities have been identified,
- With high turnover, and
- Where the self-assessment has indicated issues in the past.

Monitoring begins with the control owners, who perform a self-assessment of their key controls on a monthly, quarterly or annual basis (depending on the control's frequency) and document the results in a reporting tool that resides on the network. Management-level process owners above the control owner conduct supervisory reviews through a process they call Field Internal Control Assessments (FICA). These supervisory reviews are conducted on a frequency that is commensurate with the level of risk, and are executed from an audit program designed to test key financial and operational controls.

Use of a formalized risk assessment methodology

Example 17: A provider of Internet-based securities brokerage and financial services has a formal Corporate Risk Committee (CRC) tasked with facilitating the enterprise risk management process.

One of the key tasks of the CRC is the facilitation and completion of an Annual Enterprise Risk Assessment using the COSO ERM Framework. CRC members identify, assess, and evaluate risks across all strategic, operational, reporting, and compliance activities. Business unit leaders, who have input into the risk assessment process, are then tasked with managing or mitigating those risks within their area of responsibility. The process includes ensuring that internal control over the identified risks is designed and operating effectively (i.e., monitoring).

The business unit leaders have established monitoring procedures that are linked to the prioritized risks. The results of those procedures are reported to senior management on a regular basis. If risks change, the business unit leaders are responsible for making any necessary modifications to internal control and related monitoring procedures.

Use of a formalized risk assessment methodology

Example 18: In completing its annual Business Risk Assessment, management of a retail chain store company utilizes rational groupings of risk (i.e., “real estate,” “general accounting,” or “loss prevention”). These rational groupings are comprised of a number of discretely defined risk factors. Once risks are defined, management identifies the specific controls that mitigate the discrete risk factors. This process helps management determine what controls to monitor and how they will be monitored. After completion of the first Business Risk Assessment, the company anticipates that future updates will be more limited in scope, focusing on environmental and organizational changes over the past year and revisiting the risk assessment in areas where problems have surfaced. (See Appendix D for excerpts from this company’s risk matrix.)

2 Identify Controls

Understand the Internal Control System and Identify Key Controls

Guidance Summary: In order to identify the important or key controls to monitor, the people designing monitoring procedures must first understand (1) how the internal control system is designed to manage or mitigate the identified risks, and (2) how the control system could fail and that failure not be detected in a timely manner. Important controls — often referred to as key controls — are those that are most important to monitor in order to support a conclusion about the internal control system’s ability to manage or mitigate meaningful risks. They often have one or both of the following characteristics:

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

The discussion of key controls in this guidance is not intended to establish different classes of internal control. Rather, it is to help organizations understand how they might reasonably conclude that the internal control system is effective in addressing a given risk by focusing monitoring efforts on a subset of controls.

Example 19: The internal audit department at a financial services company builds its audit programs for corporate, departmental and individual location audits based on:

Development of an audit program based on an analysis of key controls

- An understanding of how the internal control system is designed to address meaningful risks, and
- The identification of controls within that system that are most important to addressing those risks.

Its assessment is based on its experience in the industry, knowledge of the underlying control risk, the existence of any changes, or past problems in the area.

Example 20: Management of a small manufacturing company has prioritized its monitoring procedures based on the significance and likelihood of risks and the relative importance of certain controls in mitigating those prioritized risks. In selecting “key controls” to monitor management first considers whether failure in a given control might lead to a material error.

Small manufacturing company’s consideration of key controls

Some key controls, such as the reconciliation controls over certain significant accounts, could cause an error if they fail even once. In such cases, management monitors those controls on an ongoing basis, using primarily direct information.

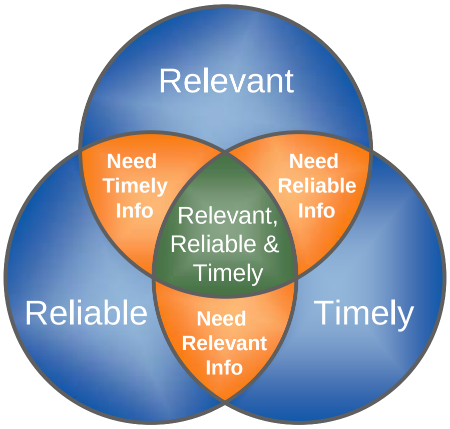
Other key controls, such as controls over the changing of depreciable lives in the fixed asset system, would have to fail over an extended period of time in order to be material. In those cases, management’s ongoing monitoring utilizes more indirect information, with periodic separate evaluations of the controls using direct information. The interval between separate evaluations is dependent on (1) management’s judgment of the level of risk, and (2) its related determination of what constitutes a reasonable interval.

Still other key controls serve to detect earlier control weaknesses before they can lead to a material error. Monitoring these key controls allow management to improve the efficiency of monitoring without impairing its effectiveness. For example, the company employs a three-way match control that compares the quantities and dollars included in purchase orders, receiving logs and invoices. This key control, if it operates effectively, would detect failures in controls over data entry in the receiving or accounts payable departments before such failures could lead to improper payments or inaccurate accounting. Accordingly, rather than frequently test controls over data entry regarding receiving or accounts payable, management focuses its monitoring efforts on the three-way match control.

Identify Persuasive Information

Guidance Summary: The **persuasiveness** of information refers to the degree to which the monitoring information is capable of providing adequate support for a conclusion regarding the effectiveness of internal controls. Persuasive information is both **suitable** and **sufficient** in the circumstances and gives the evaluator reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of the internal control system in a given risk area.

Suitability of information is a broad concept that implies that information is useful within the context for which it is intended. In order to be suitable, information must be **relevant**, **reliable**, and **timely** (See Figure 4). *Sufficiency* is a measure of the quantity of information (i.e., whether the evaluator has enough suitable information).



Elements of Suitable Information
Figure 4

Integration of operations and finance into one technology platform

Example 21: An international manufacturer implemented an integrated production and financial reporting system across the organization. This system reduces the amount of data transfer and reconciliation needed to produce operating and financial information, thus improving its reliability. As such, management is better able to monitor product quality, operational, and financial results. This improved reliability has a corresponding increase on the ability of the resulting indirect information to identify potential control deficiencies.

Use of indirect information in addressing operational risks

Example 22: An international manufacturer holds monthly meetings to evaluate operational and quality results against standard metrics that are linked to the organization's strategic objectives. Business units report their metrics and related analysis using standardized templates which include the related goal, the current status in relation to the goal and the historical performance against the goal.

Management may initiate a specific quality audit (i.e., a separate evaluation) of any process where statistical indicators show a negative trend or where it identifies, through observation or customer complaint, a potential quality issue. Business unit leaders also: execute regularly scheduled audits of production quality controls; recommend remediation; and track and report remediation of production quality issues. Finally, internal audit develops its annual plan, which includes ongoing and separate evaluations, based in part on the results of this indirect information analysis.

Balanced use of direct and indirect information in addressing operational risks

Example 23: In relation to certain operational risks at plant locations, the Vice President of Operations at a medium-sized manufacturing company has been able to make more effective use of indirect information to determine whether plant controls are operating properly. Two specific examples include controls related to labor costs and capital expenditures.

Labor — This company experiences a moderate-to-high degree of turnover at its plant locations, resulting in frequent additions to and terminations from plant payroll. The company has determined that the risk of material, operational (or financial reporting) problems in this area is relatively low, given the consistency and small dollar amounts involved on a per-person basis, and the relative simplicity of the process. As a result, the company relies on monitoring of labor variances as opposed to frequent direct testing of specific controls over additions, terminations or adjustments to payroll.

During the annual budgeting process the company determines its production plan, headcount requirements and expected overall labor costs. The VP of Operations monitors the labor variance and investigates any large or unusual items. Any increase or decrease should be commensurate with the current month's production activity and employee turnover.

Capital Expenditures — The company has controls in place to address the risk of improper capital expenditures. These controls include required approvals for purchase orders and invoices, and a three-way match of purchase orders, invoices and receiving documents.

Capital expenditures are approved as part of the annual budgeting process and allocated to the plant when incurred. Direct expenses are budgeted in accordance with the anticipated production whereas indirect expenses are budgeted based on historical trends and allocated accordingly. The VP of Operations conducts ongoing monitoring through the review of these costs and investigation of any large or unusual variances. He also meets weekly with the CEO to discuss performance and explain variances in detail.

The company has concluded that the level of operational (and financial reporting) risk is higher in this area than with labor expenses. This higher risk is due, in part, to the frequency of these transactions and the greater potential for improper expenditures to be incorporated into the budgeted amounts over time without being detected by the review of indirect information. As a result, the company supplements the ongoing monitoring of indirect information with annual direct tests of the approval controls and the three-way match. The combination of ongoing monitoring using indirect information and periodic separate evaluations using direct information has enabled the company to maximize the efficiency of its monitoring efforts related to capital expenditures while still addressing the risk in an adequate manner.

Improved use of indirect information to monitor payroll

Example 24: Approximately 90% of a medium-sized manufacturing company's employees are located at plant sites. The company implemented a new payroll software and workflow to review and approve payroll. All bi-weekly payrolls are reviewed in detail at the plant sites and submitted through the workflow. The corporate payroll manager reviews plant payrolls for unusual fluctuations, such as increase/decrease in employee headcount, excessive overtime, etc. Any identified fluctuations are reviewed and require sufficient response and support prior to payroll processing. This monitoring control allowed the corporate payroll manager to identify a plant accountant's continual excessive overtime, which occurred outside the normal monthly plant closing cycle. After further investigation, management discovered that the plant accountant had falsified overtime hours. Thus, improving upon the review of indirect information enabled this organization to identify a control deficiency and fraud in an area typically considered to be of low to moderate risk.

Implement Monitoring Procedures

Guidance Summary: Once the risks are prioritized, key controls are noted, and the available persuasive information is identified, the organization implements monitoring procedures that evaluate the effectiveness of the internal control system's ability to manage or mitigate the identified risks. Monitoring involves the use of ongoing monitoring procedures and/or separate evaluations to gather and analyze persuasive information supporting conclusions about the effectiveness of controls across all five COSO components. There may also be opportunities to improve the effectiveness and efficiency of monitoring through the use of technology.

Ongoing Monitoring and Separate Evaluations

Guidance Summary: Ongoing monitoring procedures are built into the normal, recurring operating activities of an organization. They include regular management and supervisory activities, peer comparisons and trend analysis using internal and external data, reconciliations and other routine actions. Separate evaluations are planned and performed periodically and are not ingrained in the daily operations of the organization. As such, they are not designed to evaluate controls as frequently as ongoing monitoring.

In general, as organizations increase the degree and effectiveness of ongoing monitoring, they will find less need for separate evaluations. The 1992 COSO Framework states, "An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize 'building in' versus 'adding on' controls."

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

Necessary modifications to improve ongoing monitoring

Example 25: At a retail chain store company, ongoing management monitoring of store operations has always been considered crucial to the success of the organization. However, growth in the number of stores combined with some incidents of fraud, led management and the board to invest in the development of a monitoring function at the corporate level — the Store Operations Group — to improve the ongoing monitoring of controls over store operations.

The Store Operations Group includes former store managers, district managers, auditors, and technology personnel. The team has access to real-time store operations data to perform monitoring of daily, weekly, and monthly financial and operational indicators. For more information on this retail chain store company's ongoing monitoring procedures, see the example in Chapter V titled *Large Retail Organization's Monitoring of Controls over Store Inventory*.

Effect of self-assessments in determining which monitoring procedures to employ

Example 26: The Internal Control Assessment Program (ICAP) at an Internet-based securities brokerage and financial services company serves as one form of ongoing monitoring of key internal controls (see Example 9:). As the first line of defense against control deficiencies, the presence of the ICAP allows management to concentrate its ongoing monitoring efforts on (1) areas of higher risk (absence of self-assessments would dilute monitoring efforts to include lower-risk areas); (2) areas where the ICAP has identified potential problems; or (3) areas where separate evaluations have identified control deficiencies that were not reported through the self-assessments. Thus, the organization is better able to focus its separate-evaluation efforts on a prioritized-risk basis and modify ongoing monitoring procedures where necessary.

Effect of changing risk factors on type, timing and frequency of monitoring

Example 27: A medium-sized manufacturing company has 13 different plant locations, six of which were deemed to be significant. Management planned to monitor internal control in the less significant plants, primarily through ongoing monitoring procedures including a review of monthly reconciliations and analytical reviews. However, management identified several risk factors, including frequent errors in monthly and quarterly reconciliation activities and turnover among plant-level controllers and supervisory personnel. These risk factors led management to conclude that periodic evaluation of more-direct information was necessary at its smaller plants. Accordingly, management implemented random plant audits that evaluate key controls on a periodic basis. The organization also conducted additional training of plant controllers to address the identified control deficiencies. These actions helped to improve the ongoing effectiveness of controls at the plant level.

Using Technology for Effective Monitoring

Guidance Summary: Organizations often use information technology (IT) to enhance monitoring through the use of control monitoring tools and process management tools. Control monitoring tools often operate as controls and, simultaneously, provide monitoring information on the continued operations of other controls. Process management tools automate certain activities associated with monitoring, including assessing risks, defining and evaluating controls, and communicating results. Most of these tools use workflow techniques to provide structure and consistency to the performance of monitoring procedures.

Use of a monitoring-status tracking tool and dashboard report

Example 28: A beverage manufacturer and distributor utilizes a pre-packaged reporting tool for internal controls. The tool serves as a repository for:

- Control owners to document control self-assessments and for other evaluators to document the results of their monitoring efforts;
- Documentation concerning process and control workflows; and
- Remediation plans, status and completion based on management’s plan.

The tool also provides senior management and the board with a dashboard report showing the status of monitoring procedures throughout the organization and their related results.

Use of a monitoring-status tracking tool

Example 29: A provider of Internet-based securities brokerage and financial services uses an automated tool to document its quarterly Internal Control Assessment Program (ICAP) in which business unit owners are required to execute quarterly self-assessments and certify the controls for which they are responsible (see Example 9:). This tool facilitates the planning and performance of separate evaluations that monitor the effectiveness of the ICAP process. It also serves as a reporting tool for senior management and the board.

The implementation of this tool has provided several benefits to the organization. First, the configuration of the automated tool ensures that business unit owners take ownership of controls because the system forces the owner of the control to affirm routinely that the reporting process is “complete” within the tool. Second, the automated tool includes a comprehensive control deficiency reporting feature that tracks the resolution and disposition of identified internal control issues and sends reminders and reports to appropriate personnel based on pre-defined criteria.

Continuous monitoring of segregation-of-duties controls

Example 30: A beverage manufacturer and distributor utilizes a segregation-of-duties (SOD) tool to provide continuous monitoring over SOD. This tool allows the organization to customize SOD based on established rules. The SOD tool is used as both preventive and detective tool and has allowed the organization to push accountability for SOD and system security out to the business units rather than maintaining it within IT. The tool produces a report listing all SOD conflicts that meet predefined criteria, which is reviewed by appropriately objective personnel.

Improved monitoring through the use of a reconciliation tracking tool

Example 31: The same beverage manufacturer and distributor uses a database tool to track and test all reconciliations, including their completion and review. Each general ledger account is risk-ranked based on materiality, complexity, issues identified in the prior year, change in environment, risk for fraud, etc. Management uses this risk assessment, and any anomalies flagged by the tracking tool, to direct its independent testing and review of the reconciliations. In the past, the organization would test, through separate evaluations, both the preparation and the approval controls for the reconciliations. The implementation of this tool allows the organization to monitor the completion and review of reconciliations more efficiently.

Continuous monitoring using conditional tests of transaction data

Example 32: A large power generation organization has implemented automated tools to perform daily, weekly, and monthly compliance monitoring. These tools include conditional tests that match transaction data against predefined parameters outlined and identified in the corporate trading policy manual.

The tool assigns a level of severity to identified anomalies based on established risk policy standards, and automatically notifies the people responsible for addressing the issue. Identified exceptions to the trading policy are tracked by the trading risk manager and a monthly summary of violations is presented to the organization Risk Oversight Committee (ROC). Significant violations are specifically discussed with both the ROC and Audit Committee.

The use of this tool does not preclude the use of manual monitoring techniques, but it does influence the type, timing and extent of manual monitoring.

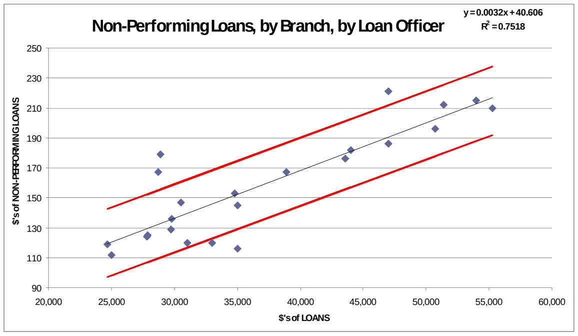
Continuous monitoring using conditional tests of transaction data

Example 33: A large manufacturing company was using a labor-intensive separate-evaluation approach to monitor controls in the company’s procure-to-pay processes. In order to improve the efficiency and effectiveness of the monitoring process the company implemented a commercially-available continuous monitoring tool. The tool uses advanced analytics, incorporating a library of 130 pre-defined integrity checks that are consistent with those used by forensic accountants, auditors and fraud examiners to identify fraud, misuse and errors in the procure-to-pay cycle. The tool monitors each transaction and flags potential control exceptions for review. Implementing the tool enabled the company to uncover control violations including improper and duplicate transactions. It also allowed the organization to streamline and tailor its separate evaluations to serve more efficiently as periodic confirmation of the effectiveness of the ongoing monitoring procedures.

Continuous monitoring using regression analysis

Example 34: Many financial institutions employ continuous control monitoring tools in areas such as (1) loan granting/management, (2) loan provisioning/performance, (3) money laundering, (4) counterfeit checks, (5) Suspicious Activity Reporting (SARs) and resolution, and (6) wire transfer anomalies.

One financial institution developed a simple regression analysis of non-performing loans by branch, by loan officer (see the figure below) as one form of monitoring indirect information related to controls over loan origination. The red statistical precision intervals allow the organization to look for outliers across multiple metrics (e.g., policy, industry standards or statistical standard deviations). Further, the report can be re-populated in either real-time or batch mode. This analysis helps the organization identify loan officers and/or branches that may not be following loan origination policies.



IV. Assessing and Reporting Results

Guidance Summary: The monitoring process is complete when the results are compiled and reported to the appropriate personnel. This final stage enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control, or highlight identified deficiencies for possible corrective action.

Prioritizing and Communicating Results

Guidance Summary: Consistent with Principle 20 of COSO's 2006 Guidance, effective monitoring includes identifying control deficiencies and communicating them to the right people in a timely manner. Some organizations accomplish this goal by ranking identified control issues by severity along a continuum such as high, medium, or low, or along a numerical scale (e.g., 1–5 or 1–10). Other organizations use a less formal mechanism.

Use of a tool to help prioritize, track and report potential deficiencies

Example 35: An international manufacturing company developed a custom Access database to track production quality issues — those identified both externally from clients and internally from management's monitoring and Quality Audit reviews. Issues are prioritized, logged, traced to a root cause, assigned to a manager within the production area, and tracked until the issue is resolved.

Management receives a presentation from the Production Quality Audit Team leader regarding the status of open quality issues on a monthly, quarterly, and annual basis. Significant issues that may impact the ability of the business to achieve its operational, financial, and quality objectives receive special attention from business unit leadership and are reported to executive management during their monthly, quarterly, and annual meetings.

Executive management of the organization requires business unit and functional leaders not only to test and report results to management, but also to certify the controls for which they are responsible (see Appendix B).

Use of a tool to help prioritize, track and report potential deficiencies

Example 36: Senior management of trading operations at a large power generation organization reviews all trading policy violations and assigns a level of severity for each violation based on criteria defined in the Trading Risk Policy. The organization uses an automated reporting system that is integrated with the trading platform to ensure that identified issues are reported to the appropriate level for follow-up. Notification routing varies from the individual's direct supervisor, or in the case of more severe issues of non-compliance, Executive Management, Risk Oversight Committee (ROC) Members, and Internal Audit.

Factors considered in ranking identified control deficiencies

Example 37: A large government agency has a senior-level internal control working group that prioritizes remediation efforts for identified control deficiencies. In doing so, the group considers factors such as: the internal control risks, past internal control assessments and experience with other federal agencies.

Use of people trained specifically to evaluate the severity of potential deficiencies

Example 38: Management of an international manufacturer has created a Quarterly and Annual Disclosure Committee (QADC) that is responsible for performing a review and analysis of controls monitoring. An important component of this review is the quarterly and annual representations from line management, which includes representations related to the operation of internal controls (see Appendix B). Additionally, the Disclosure Committee utilizes a checklist (see Appendix C) to ensure that monitoring occurs in areas of meaningful risk.

Reporting Internally

Guidance Summary: Reporting protocols vary depending on the purpose for which the monitoring is conducted and on the severity of the deficiencies. Typically, the results of monitoring conducted for purposes of evaluating an organization's entity-wide objectives are reported to senior management and the board. Control deficiencies should be reported to the person directly responsible for the control's operation and to at least one management level higher that has oversight responsibilities. Reporting at least to these two levels gives the responsible person the information necessary to correct control operation and also helps ensure that appropriately objective people are involved in the severity assessment and follow-up.

Established reporting protocols for identified deficiencies

Example 39: The Internal Audit Department at a medium-sized manufacturer logs and tracks all identified control deficiencies and assesses their impact to the organization. These control deficiencies are reported to the management team responsible for the audited business unit. An individual within the business unit is assigned responsibility for remediation of specific control deficiencies. Internal Audit assigns a remediation timeframe for each identified control deficiency based on that specific deficiency's ranking. Deficiencies must be remediated within the specified timeframe or a clear plan must be in place to address the deficiency.

Use of a spreadsheet to track and report deficiencies

Example 40: The Store Operations Group at a retail chain store company tracks identified control deficiencies on a spreadsheet until they are resolved. These issues are communicated to executive management and the Audit committee on a quarterly basis.

Established grading scale and reporting protocol for identified deficiencies

Example 41: At an international insurance services organization, the Internal Audit Department classifies control deficiencies identified during the course of an audit as: Minor Deficiencies, Reportable Deficiencies, and Significant Deficiencies. The communication structure for reporting deficiencies is based on the deficiencies' potential impact to the organization. The Company's internal reporting structure requires that:

- Minor Deficiencies — are reported at the end of each audit, in detail, to the manager responsible for the control.
- Reportable Deficiencies — are reported at the end of each audit, in detail, to the manager responsible for the control and to the senior management team and on a quarterly basis, in summary, to the Audit Committee.
- Significant Deficiencies — are reported at the end of the audit, in detail, to the manager and the senior management team and on a quarterly basis, in detail, to the Audit Committee.

Reporting Externally

Guidance Summary: Many organizations are required to report to third parties on the effectiveness of their controls. A properly designed and executed monitoring program helps support external assertions because effective monitoring provides persuasive information that controls operated effectively during the period.

Potential Modifications to Monitoring

Guidance Summary: Effective monitoring procedures generally provide substantial support for external reporting requirements regarding internal control effectiveness. However, modifications to the monitoring program in some areas may be warranted or beneficial to the organization when external reporting is required. For example, assume that, in a given risk area, an organization uses less objective forms of monitoring (such as self-evaluations) for internal purposes. The organization may find that increasing the evaluator's objectivity allows the external auditors to use more of his or her work in the conduct of their audit, thus improving overall efficiency.

Benefits of joint planning between the organization and the external auditor

Example 42: Senior–management and the Internal Audit department of a small financial institution hold an annual audit planning meeting with the external auditor. They discuss management's approach to the evaluation of internal control over financial reporting and consider modifications to that approach in areas where doing so might increase the external auditor's ability to use the work of management and/or internal audit in the conduct of their external audit procedures. For example, internal audit decided to increase slightly its sample size of control tests in a few key areas in order to provide a large enough sample to meet the external auditor's needs.

Consideration of the use of external specialists

Example 43: For several years, an international manufacturer has utilized external specialists to perform separate evaluations of controls over various aspects of the organization. Use of these specialists is determined by management based on (1) the results of the annual risk assessment process, (2) consideration of the external auditor's needs and its ability to use the work of these specialists in conducting its audit, and (3) the capabilities of the organization's internal audit staff. Results and issues identified by these specialists are reported and tracked internally.

V. Comprehensive Examples

The brief examples presented in Chapters II–IV of this volume are intended to demonstrate how different organizations might apply the concepts set forth in the Guidance (Volume II). Their brevity provides an easy reference point for specific concepts, but it does not provide a comprehensive look at monitoring a given risk from beginning to end.

This chapter provides three comprehensive monitoring examples that flow from the point at which a given risk is assessed, through the monitoring process, and, ultimately, to the execution of monitoring procedures and the reporting of results to management and the audit committee. The first two examples — one of a large retail organization and the other of a mid-sized manufacturing company — are live examples of monitoring in two organizations. The third example is compiled from project team members' experiences in helping companies monitor information technology risks effectively and efficiently.

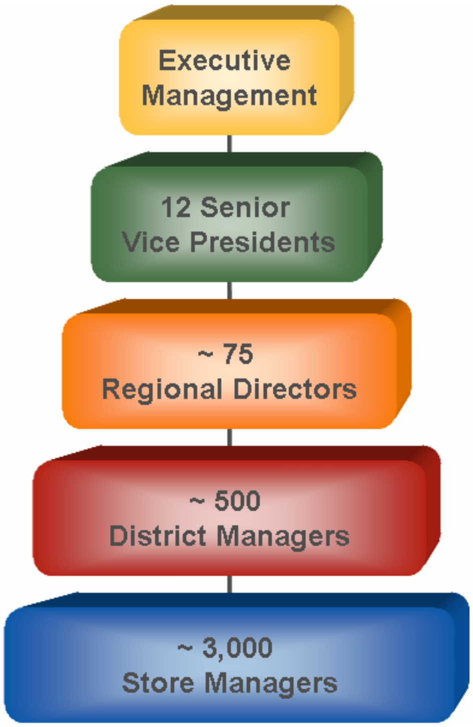
Table of Contents

Large Retail Organization’s Monitoring of Controls over Store Inventory

Background Information

1. A large retail organization has in excess of 3,000 store locations and a tiered management structure for store operations, including:

- Executive management,
- 12 senior vice presidents (SVPs) each of whom oversees approximately 6 regional directors,
- Approximately 75 regional directors each of whom is responsible for 6–8 districts,
- Approximately 500 district managers each of whom is responsible for 6–8 stores, and
- Individual store managers for each location.



2. Internal control monitoring takes various forms at every level of management. This example will concentrate on risks associated with managing store inventory, which management has determined are important to the organization from both an operations and a financial reporting standpoint.

3. The primary responsibility for internal control of store operations rests with store managers. Through procedures performed during store visits that occur at least monthly, district managers perform the most direct monitoring of the continued effectiveness of controls in individual stores. Regional directors and other members of management also visit stores periodically; however, their primary monitoring procedures involve the review of detailed store statistics (i.e., indirect information that might identify a store with internal control issues affecting operations and financial reporting) and their interactions with, and observations of, district managers.

4. The large size of the organization and the fact that its 3,000+ stores are statistically comparable make it a practical candidate for maximizing the use of monitoring using indirect information. Thus, the senior vice presidents and members of executive management monitor many controls, including store-level inventory controls, through extensive ongoing monitoring of store operating statistics.

5. Over time, growth in the number of stores placed stress on the previous approach to monitoring store operations that consisted primarily of infrequent visits by the Internal Audit function. As a result, management performed a comprehensive review of the organization's internal control over store operations (establishing a baseline of effective internal control) and made three significant changes to the underlying monitoring structure. First, it shifted much of the monitoring responsibility to store managers and district managers. Second, it enhanced the detail contained in operational reports reviewed by managers at all levels. Third, it invested in the development of a monitoring function at the corporate level — the Store Operations Group (SOG) — to enhance both the underlying control activities and the ongoing monitoring of controls at the store level.

6. The SOG comprises former store managers, district managers, auditors, and technology personnel. The employee mix provides the group with both competence and objectivity in performing its monitoring duties. Furthermore, to enhance its objectivity, the SOG is part of the organization's internal audit function rather than part of operations or corporate finance. As discussed later, however, the SOG does report potential internal control issues to appropriate personnel outside of internal audit.

7. The SOG accesses real-time store-operations and financial data to perform standard daily, weekly, monthly, quarterly, and annual reviews of store-level

financial and operational data. Using its extensive knowledge of store operations, risks, and related controls, the SOG designed custom database reports to cover key areas of operations and internal control, including information related to:

- Execution of weekly and monthly store inventory audits,
- Late-deposit activity,
- Cash-drawer activity,
- Inventory adjustments due to theft, spoilage, and customer charge-offs,
- Inventory purchasing and item-receipt activity, and
- Pricing overrides.

Understanding and Prioritizing Risks

8. On an annual basis, the organization completes a comprehensive, enterprise-wide risk assessment. Those involved in the assessment include senior management, business unit leadership, and where appropriate, direct reports of business unit leaders. The focus of this risk assessment is identifying the effect and probability (sometimes referred to as "significance and likelihood") of financial, operational, and compliance risks at the store-operations and corporate levels. Risks are scored numerically from a low of "1" to a high of "5" and support the judgmental prioritization of the risks. Once prioritized, the risks are broken down further into levels — or "risk factors" — that indicate how the risks might manifest. The table below shows how the organization groups and prioritizes risks.[4]

9. Overall, management recognizes that effective store inventory management is crucial to the organization's operations and financial reporting objectives. As a case in point, we will follow one of those risk factors, "Inaccurate/improperly adjusted store inventory balances" (risk factor 2.b. below), through the monitoring process.

10. This organization sells primarily furniture, appliances, and electronics. Inventory items are generally large, which means they are easy to count for inventory purposes, and are more difficult to steal than inventory items at other retailers, such as clothing stores or department stores. However, if pervasive theft or shrinkage exists across multiple locations, or if store managers are able to

[4] Some organizations may choose to conduct their risk prioritization efforts at the level this organization refers to as "risk factors." For this organization, however, prioritizing the risks one level higher, and then focusing on the controls that address the related risk factors, provides an adequate level of support for their internal control decisions, including what and how they will monitor internal control.

fraudulently misstate inventory balances, such deficiencies could lead to errors that, in the aggregate, would be material to the organization both in terms of its operational goals and the accuracy of its published financial statements.

11. Knowledge of these factors, along with management's understanding of the organization and its business, provides support for the organization's inventory-related risk assessment process. The following table exemplifies the organization's more detailed risk assessment process for inventory.

Risks	Risk Factors (i.e., What Can Go Wrong)	Impact Ranking	Probability Ranking	Priority
1. Inappropriate product type/quantity mix, inventory levels, or store purchasing	a. Revenue loss due to inability to meet customer demands b. Carrying excess store inventory c. Write-offs from stale/obsolete inventory	5	3	H
2. Inappropriate/ inaccurate/untimely inventory-level reporting	a. Not identifying damaged/obsolete inventory b. Inaccurate/improperly adjusted store inventory balances	5	3	H
3. Inappropriate store-level inventory receipt	a. Inventory not being recognized/recorded in the system in a timely fashion b. Inadvertent acceptance of damaged/obsolete inventory c. Improper inventory costing d. Hard/soft expense associated with correcting delivery errors e. Increased theft/damage risk due to re-deliveries	3	3	M
4. Inventory theft	a. Direct financial loss b. Overstatement of inventory balances c. Understatements of expenses/overstatements of net income	3	3	M
5. Inaccurate/untimely store-to-store inventory transfers	a. Revenue loss due to inability to meet customer demands b. Carrying excess store inventory c. Inaccurate store inventory balance d. Inability to perform accurate store inventories	5	3	H
6. Inaccurate/ unavailable store	a. Revenue loss due to inability to meet customer demands	5	1	M

Risks	Risk Factors (i.e., What Can Go Wrong)	Impact Ranking	Probability Ranking	Priority
inventory data	b. Inaccurate inventory booking and costing adjustments c. Poor information for purchase price negotiations d. Inability of store managers and district managers to perform scheduled inventories accurately			

Understanding the Internal Control System and Identifying Key Controls

12. Once management has prioritized the risks related to inventory management, the organization links those risks to controls that address them. This process sets expectations for store operations management, corporate finance, and internal audit regarding how the internal control system should manage or mitigate identified risks.

13. Management further refines monitoring efforts by identifying which of the controls are most important to monitor in order to conclude that the internal control system is properly managing or mitigating the prioritized risks.

14. In regards to "Inaccurate/improperly adjusted store inventory balances" risk, management has implemented a number of controls:

- *Periodic inventory* — To ensure accurate inventory counts at the store level, the following inventory-count procedures are performed:[5]
    - The store manager is required to perform a bar-code inventory (i.e., electronically scanning the bar codes of items in inventory) three times per week on Monday, Wednesday, and Friday. As it is taken, the inventory is automatically recorded in the centralized information system.
    - The store manager is also required to perform a monthly serial-number inventory (i.e., counting inventory by serial number and comparing with inventory records).
    - The district manager is required to perform a monthly serial-number inventory.

[5] These extensive store-inventory controls are possible because inventory consists of a relatively small number of large items that are easily counted. The scope of these controls may not be feasible in other types of organizations, including other retail organizations.

  - Store managers conduct their inventories using barcode scanners that automatically document the results within the centralized information system. Inventories are also timed within the system so that management can monitor how long it takes to conduct specific inventories and react accordingly. Inventories that are performed too quickly may indicate a rushed and ineffective inventory count; inventories that take too long may signal a need for training or other operational improvements.

- *Restricted access to record adjustments* — To ensure proper oversight and approval of adjustments to inventory balances, only the district manager is able to record inventory adjustments for spoilage, theft, or customer charge-offs.

- *Monthly analytical review* — To mitigate risk of inappropriate store-level inventory management and to assess overall store-level profitability, all inventory adjustments are reviewed during monthly district manager and regional director profit and loss (P&L) reviews. Trends in the same store over time are analyzed and compared with those of other stores across a wide variety of key performance indicators.

- *Daily inventory report review* — To ensure that store-level inventory activity is accurate, the district manager reviews a daily report that shows inventory balances on hand, inventory item receipt, open purchase orders, and inventory-count exceptions.

- *Exception report review* — To ensure that inventory counts are performed on a timely basis, the SOG, district manager, and regional director are notified if inventory counts have not been completed in the system for two weeks.

- *Supervisory store audits* - To ensure that store inventory counts are executed properly and that store managers are effectively addressing idle inventory, the district manager performs comprehensive quarterly store audits. Relative to inventory risk, these store audits include a review of completed store-manager inventory counts, identification and execution of inventory adjustments, and an assessment of idle inventory (i.e., inventory idle for more than 90 days). The conduct of the quarterly store audits is documented in the centralized information system, and the audit results are reviewed by the SOG and reported to the applicable regional director.

15. Note that no individual store’s inventory could be so wrong that it becomes material to the organization as a whole, even if it were 100 percent wrong. A pervasive failure of the store-manager inventory control, covering multiple district managers, would have to occur before such a risk could become material to the

organization as a whole. Therefore, by focusing monitoring efforts at the store level, and by spreading the risk of control failure across numerous district managers, the organization effectively reduces the potential for inventory control failures to become material to the organization. These organizational factors are important in considering the type and amount of persuasive information necessary to support a conclusion that the internal control system is effective in relation to the risk.

Identify Persuasive Information About the Execution of Inventory Controls

16. Relative to the identified risk (i.e., inaccurate/improperly adjusted store inventory balances), the store managers' tri-weekly and monthly inventory counts are the key controls designed to ensure the accuracy of inventory balances in the system. With the exception of the control restricting access to record adjustments, all other controls identified by management provide various levels of monitoring to ensure that (1) the store managers' periodic inventories are performed accurately, or (2) inventory balances and adjustments appear reasonable on a store-by-store basis. In this particular organization, management personnel at each level of the organization seek to identify sufficient relevant, reliable, and timely information to indicate whether store inventory control is working and inventory balances are accurate.

17. Because of the organization's size and tiered management structure, executive management's monitoring efforts (in this case, the CFO's monitoring efforts) depend on (1) the effectiveness of monitoring at the SVP, regional-director and district-manager levels, (2) the effectiveness of monitoring performed by the SOG, and (3) executive management's own ongoing monitoring of store statistics across the organization.

Direct Information

18. Available relevant, reliable, and timely direct information regarding the operation of the store managers' tri-weekly and monthly inventory counts includes the following components:

- System records detailing the date, time, and results of the store managers' inventories,
- The district managers' direct observation of store managers taking inventories, and
- The results of the district managers' own monthly inventories, which would identify the failure of any given store manager's inventory count before that failure could contribute to a material error.

Indirect information

19. Available indirect information that may indicate a potential failure in the store-manager inventory controls includes the following components:

- Detailed store-level metrics that show store trends and comparative metrics including product-level analyses, cost of goods sold, profitability, etc.,
- System records detailing the duration of each inventory count, and
- Store-level inventory records in the system, including on-hand balances, inventory items received by the store, open purchase orders and any needed adjustments to inventory balances based on inventory counts.

Implementation of Inventory Controls Monitoring

20. The following table highlights how various levels of management monitor the effectiveness of the store-manager inventory controls, beginning with the district manager and ending with the CFO. Note that all of these monitoring procedures, including the separate evaluations, are part of the organization's normal operating activities. The procedures were not developed solely to meet an established regulatory requirement.

Monitoring Procedure	Information Type	Monitoring Type	Comments
District Managers			
1. Review daily store-level inventory report.	Indirect	Ongoing	This report enables the district manager to gauge quickly whether inventory balances are reasonable now and in the near future. It also gives the district manager an idea of what inventory should be on hand when he or she visits the store.
2. Conduct monthly store inventory by serial number.	Direct	Ongoing	This procedure serves as both a control activity (identifying errors in the inventory balances) and a monitoring procedure (re-performing, and thus validating, the store manager's inventory control).

Monitoring Procedure	Information Type	Monitoring Type	Comments
3. Conduct monthly store-level analytical reviews between the district manager and the regional director.	Indirect	Ongoing	Through this monthly analytical review, the district manager and regional director can identify inventory anomalies that warrant further investigation.
4. Conduct quarterly store audits, including an examination of store-manager inventory records.	Direct	Separate Evaluation	This monitoring procedure provides for periodic examination of store operations, including inventory management, at a detailed level that revalidates the effective operation of internal control.
5. Follow up on any inventory exceptions identified by the SOG.	Direct	Separate Evaluation	If the SOG identifies a store that either has not taken a required inventory in two weeks (see the SOG below) or presents other anomalies identified through analysis, the district manager and regional director are notified so that they can follow up on the exception.
Regional Directors and Senior Vice Presidents			
1. Review daily, weekly, and monthly store operating reports that highlight numerous statistics relevant to inventory levels, cost of goods sold, and profitability.	Indirect	Ongoing	This report enables the district manager to gauge quickly whether inventory balances are reasonable now and will be in the near future. It also gives the district manager an idea of what inventory should be on-hand when he or she visits the store.
2. Discuss store operations, including inventory management, during regularly scheduled operational meetings between the SVPs and their regional directors, and between the regional directors and their district managers.	Indirect	Ongoing	This discussion, while high-level given the number of stores, gives regional directors and SVPs an opportunity to inquire about stores and store managers that may not be as effective as others.

Monitoring Procedure	Information Type	Monitoring Type	Comments
3. Periodically visit store locations.	Indirect	Separate Evaluation	Regional directors and SVPs are unable to visit a large number of stores or to conduct or observe the inventory controls in action. Nonetheless, periodic visits send an important message to the field about the importance of internal control. They also enable the regional directors and SVPs to see firsthand the quantity and condition of inventory on hand.
4. Follow up on any inventory exceptions identified by the SOG.	Direct	Separate Evaluation	If the SOG identifies a store that either has not taken a required inventory in two weeks (see the SOG below) or presents other anomalies identified through analysis, the district manager and regional director are notified so that they can follow up on the exception.
Store Operations Group			
1. Perform detailed store-by-store analytical reviews, examine exceptions, and report results to management.	Indirect	Ongoing	This detailed analysis provides an objective, educated review of store-level statistics that has a high likelihood of identifying problem stores before they can contribute to a material error. The SOG developed its list of key indicators based upon professional experience and with assistance from dedicated technology personnel who “mine” corporate databases to gather and evaluate the applicable data. On a monthly basis, this list of key indicators and the results of the monitoring performed by the SOG are reviewed by internal audit, store operations executive leadership at the home office, and the organization’s executive committee.
2. Review evidence in the information system of the completion and results of the store managers’ tri-	Direct	Ongoing	Store-manager inventories are taken by electronically scanning the unique bar code on each item in stock. The SOG receives direct information from the

Monitoring Procedure	Information Type	Monitoring Type	Comments
weekly bar-code inventory.			system telling it when the inventory was completed, its duration, and its results. The SOG then compares these results with those from the other 3,000+ stores in order to spot potential anomalies.
3. Perform store-level audits of inventory and inventory controls, if necessary.	Direct	Separate Evaluation	Internal audit and the SOG have the ability to conduct separate evaluations of inventory controls, if necessary.
Chief Financial Officer			
1. Review weekly statistical reports highlighting stores with potential inventory or profitability issues.	Indirect	Ongoing	The weekly statistical report gives the CFO frequent and detailed information about the results of operations. It also highlights possible anomalies that he or she can discuss with other members of management and operations.
2. Discuss store operations, including inventory management, during regularly scheduled operational meetings.	Indirect	Ongoing	Like the discussions between the SVPs and their regional directors, and those between the regional directors and their district managers, the CFO's participation in regular operational meetings provides him or her with much indirect information about the effectiveness of store management controls.
3. Review reports from internal audit and the SOG regarding the results of their monitoring procedures.	Direct and Indirect	Separate Evaluation	In most organizations, reports from internal audit consist primarily of direct information. In this organization, however, most of the monitoring performed by the SOG is indirect. One exception is information derived from the store managers' tri-weekly bar-code inventory, which consists of direct information about stores that have not conducted proper tri-weekly inventory counts. Given the nature of the organization (i.e., a large number of homogeneous

Monitoring Procedure	Information Type	Monitoring Type	Comments
			locations that are statistically comparable), and the monitoring using direct information that takes place elsewhere in the organization, the CFO's monitoring procedures provide him with adequate support to determine whether the store-manager inventory controls are effective across the organization.

Communicating Results

21. Internal control issues identified by the district managers are normally corrected through communication between the district manager and the store manager.

22. If a store manager does not perform an inventory count over a two-week period, the SOG team is alerted to the lapse during a review of its statistical reports. After receiving this alert, the SOG team notifies the store manager directly and requests an explanation for failing to perform the inventory. The district manager and regional director responsible for the store are also notified. In addition, the issue is documented on a Store Operations Recap Report, which serves as a clearinghouse for all exception items identified by the SOG.

23. The Store Operations Recap Report is sent monthly to the Director of Internal Audit and the organization's Executive Committee. Items included in the report are maintained there until the item is considered "cleared" by the SOG.

24. In one instance, during a review of its statistical reports, the SOG identified a store that had an abnormal level of late deposits and cash drawer shortages. The SOG also noted abnormalities in several key store metrics that could be signs of fictitious customers and inventory manipulation. Those metrics included a lapse in the store manager's tri-weekly inventory counts for over 100 items, unusual fluctuations in the number of new sales contracts and new customers, a high level of past-due accounts and abnormal fluctuations in collections and profit margins.

25. The district manager responsible for the store and the organization's Loss Prevention team (a separate group within corporate operations responsible for investigating inventory-shrinkage issues) were apprised of the issues in question. Through a store visit and investigation, the district manager and the Loss Prevention team discovered that the store manager was stealing cash from the cash drawer and covering the shortage by recording sales on credit to fictitious customers, thereby removing the item from the store's inventory records. The

store manager would then sell the off-the-book inventory item for cash, which was used to cover (1) the cash-drawer shortage, and (2) the balances due from the fictitious customer. The store manager would keep any remaining cash.

26. The fraud was discovered because the SOG evaluated persuasive information that a key control focused on inventory counts was not operating effectively, as well as other indirect information that identified unusual activity. Additionally, the SOG was competent and objective, which enabled it to understand the implications of the failure of this control. By communicating/reporting this control failure to the appropriate parties through proper channels, the SOG was able to perform further investigative procedures and identify and correct the source of the problem.

27. This type of fraud, which occurs often in large retail organizations, would likely have been discovered at some point either through increased receivable write-offs or through controls related to extending credit. However, because of the robust monitoring procedures in place, the organization was able to identify the fraud quickly, take appropriate corrective action, and reduce the potential loss in a timely manner.

Supplemental Details Regarding the Above Example

The following provides some of the specific details of reports that the organization used in monitoring. This is intended as a supplement to the discussion above for those who would like to understand the process in greater detail.

Using the following report, the SOG noted an unusually high level of late deposits and cash drawer shortages.

Store #	ItemTran	Dollar	Debit	Tran	Recon Date	Account	Days Late
1749	4/6/2007	801.00	D	CD	4/23/2007	7751764167	0
1749	4/6/2007	43.58	C	SHRT	4/23/2007	7751764167	0
1749	4/9/2007	757.42	C	175	4/23/2007	7751764167	0
1749	4/14/2007	45.25	D	OVER	4/23/2007	7751764167	2
1749	4/14/2007	2,638.58	D	CD	4/23/2007	7751764167	2
1749	4/18/2007	45.00	D	695	5/1/2007	7751764167	0
1749	4/18/2007	45.00	C	SHRT	5/1/2007	7751764167	0
1749	4/18/2007	2,638.58	C	175	4/23/2007	7751764167	2
1749	4/29/2007	796.07	C	SHRT	7/20/2007	7751764167	1
1749	4/29/2007	1,740.00	D	CD	7/20/2007	7751764167	1
1749	5/1/2007	943.93	C	175	7/20/2007	7751764167	1
1749	5/4/2007	582.10	D	CD	7/20/2007	7751777167	0
1749	5/5/2007	363.90	D	OVER	7/20/2007	7751764167	0
1749	5/5/2007	1,122.33	D	CD	7/20/2007	7771764167	0
1749	5/7/2007	512.71	C	175	7/20/2007	7771764167	0
1749	5/7/2007	364.00	C	175	7/20/2007	7751764167	0
1749	5/7/2007	1,191.62	C	175	7/20/2007	7751764167	0
1749	5/16/2007	329.86	C	6280	5/17/2007	0080262008	0
1749	5/16/2007	329.86	D	455	5/17/2007	0080262008	0
1749	5/21/2007	485.42	D	BC	7/20/2007	0080262008	0
1749	5/21/2007	786.95	C	SHRT	7/20/2007	7751777167	0
1749	5/21/2007	3,930.93	D	CD	7/20/2007	7751764167	0
1749	5/22/2007	421.43	D	BC	7/20/2007	0080262008	0
1749	5/22/2007	80.00	C	SHRT	7/20/2007	0080262008	0
1749	5/22/2007	740.70	D	BC	7/20/2007	0080262008	0
1749	5/24/2007	1,567.55	C	142	7/20/2007	0080262008	0
1749	5/25/2007	3,143.98	C	175	7/20/2007	7751764167	0
1749	6/5/2007	924.05	C	CD	7/6/2007	7751764167	4
1749	6/6/2007	1,133.05	D	D	7/6/2007	7751764167	4
1749	6/6/2007	79.63	D	D	7/6/2007	7751764167	4
1749	6/8/2007	148.03	D	SHRT	7/6/2007	7751764167	4
1749	6/8/2007	643.75	C	CD	7/6/2007	7751764167	4
1749	6/11/2007	341.59	D	175	7/6/2007	7751764167	4
1749	6/11/2007	487.05	C	175	7/6/2007	7751764167	4
1749	6/11/2007	1,153.06	C	175	7/6/2007	7751764167	4
1749	6/11/2007	650.75	C	175	7/6/2007	7751764167	4

Supplemental Details Regarding the Above Example

The SOG noted that there was a pattern of both late deposits and cash drawer shortages that could indicate internal control problems related to cash, but not necessarily related to inventory. These anomalies in the cash area warranted additional investigation, and in fact, the SOG professional responsible for reviewing the above report initiated inquiries into the cause of the late deposits and cash shortages.

Soon after the above cash related items were identified, the SOG noted, from the *Weekly Bar Code Inventory Exception Report*, that more than 100 items had not been inventoried. The SOG also noticed unusual fluctuations in certain key performance indicators. The table below shows five of those indicators out of a report that covers 35 different metrics. The shaded numbers represent anomalies that warranted further evaluation.

Metric	Avg	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar
Agreements gained	6.92	-11	46	36	13	49	1	-32	11	-16	27	21	3	-58
More than 10 agreements gained is a red flag if not supported by a company promotion. Large fluctuations between months are also red flags.														
Customers gained	12.46	6	31	25	6	42	11	-4	22	3	17	21	12	-30
Significant increases in a month can be an indicator of fictitious customers. Repeated decreases can be a sign of customer service problems.														
Average past-dues	11.97	13.47	11.62	13.77	12.88	12.99	9.32	9.67	9.49	11.12	12.2	14.67	12.55	11.92
Average past-dues greater than 6% can be an indication of fictitious accounts or poor credit extension procedures.														
Percent of income colleted each month	92.14	96.30	86.50	87.20	92.00	95.00	90.50	95.10	99.10	93.10	85.50	89.80	92.60	95.10
Large fluctuations between months are a red flag.														
Monthly profit percent	5.92	-0.60	7.50	19.00	-4.00	17.00	-1.50	-0.40	17.20	11.50	-13.10	12.60	10.30	1.50
Large fluctuations between months are a red flag.														

Supplemental Details Regarding the Above Example

The cumulative effect of the above analyses lead to a separate evaluation of the controls over cash and inventory at this particular store, which uncovered the fraud in a timeframe that allowed the organization to address the problem before it could become material.

In analyzing the effectiveness of the monitoring, this example illustrates that the company started with a baseline of effective internal control. Over time they developed detailed analysis using both direct and indirect information that could identify potential problem areas in a timely manner. Moreover, there was a culture of “follow-up” in the organization that led to the timely investigation of potential problems.

Observations

28. A brief example such as this cannot convey fully the organizational context in which these internal controls, including monitoring, were developed. The personnel involved in assessing risk, designing controls and related monitoring procedures, and overseeing the internal control system have extensive experience in this organization and in this industry. Accordingly, they have developed and implemented monitoring procedures that provide information they believe to be suitable and sufficient regarding the effectiveness of the underlying controls. They continue to refine those procedures as risks and controls change.

29. Nevertheless, the project team has observed possible modifications to the monitoring procedures described in this example that may be helpful to other organizations as they consider the possible applications to their own, unique circumstances. The key for each organization is to implement internal control, including monitoring, that adequately manages or mitigates meaningful risks to organizational objectives in a cost-effective manner.

30. First, some of the monitoring performed by the district managers (e.g., taking a monthly store inventory at 6–8 stores) may seem excessive to some organizations. Because the store managers' tri-weekly inventory is recorded electronically through a bar-code scanner, the district manager may be able to review a system report documenting the results of the store managers' inventory, then conduct a separate inventory on a less frequent basis.

31. Second, above the district-manager level, little direct information is used in monitoring. Because this organization has a large number of statistically comparable stores, it is better able than many other organizations to use indirect information to identify possible control problems. Over time, though, that indirect information can become clouded by other factors. In some cases, pervasive internal control problems can gradually influence the indirect information so that even material errors appear normal. However, the persuasiveness of the information used in monitoring may be improved in a cost effective manner.

32. In this organization, if the district managers conduct their monitoring procedures correctly, there would be virtually no opportunity for pervasive control problems to develop at the store level that could be material to the organization's objectives. Accordingly, management above the district manager level, including executive management, might benefit from periodic objective monitoring — possibly through internal audit — of the district managers' monitoring procedures.

33. Objective monitoring might examine only a group of district managers each year, or select them randomly, but it would provide management with direct information supporting a belief that the district managers are performing their

duties effectively. It could also serve as additional encouragement for the district managers to execute their control responsibilities properly.

Summary and Conclusion

34. This retail organization improved both the effectiveness and efficiency of its internal control system by taking steps that are consistent with the guidance outlined in Volume II. In responding to certain identified control failures and recognizing that existing monitoring procedures were not achieving their objectives, management first performed a comprehensive review of control over store operations. It then:

- Identified and prioritized risks to its operations and to its financial reporting and compliance objectives,
- Improved the internal controls where necessary and identified key controls to monitor at various levels,
- Identified persuasive information (both direct and indirect) that would provide support for a conclusion regarding the effectiveness of the internal control system, and
- Developed monitoring procedures throughout all levels of management to evaluate the information through a mix of ongoing monitoring and periodic separate evaluations — all with an emphasis on ongoing monitoring procedures.

35. Other organizations — even organizations similar to the one in this example — may follow similar general principles, yet implement different controls and different monitoring procedures. The guidance contained in Volume II is not intended to lead every organization to the same conclusions regarding what risks are meaningful, how the risks should be controlled, or how internal control should be monitored. However, it does provide an outline any organization can use to develop monitoring procedures that will support the organization’s conclusions about the effectiveness of internal control.

Monitoring of Controls over Certain Operational Risks in a Mid-Sized Manufacturing Organization

Background Information

1. A mid-sized manufacturing organization produces complex equipment and engine components. These components typically operate for extended periods (up to 40 years) and have very low tolerance thresholds for failure. In fact, the failure of some components can have life-threatening consequences.

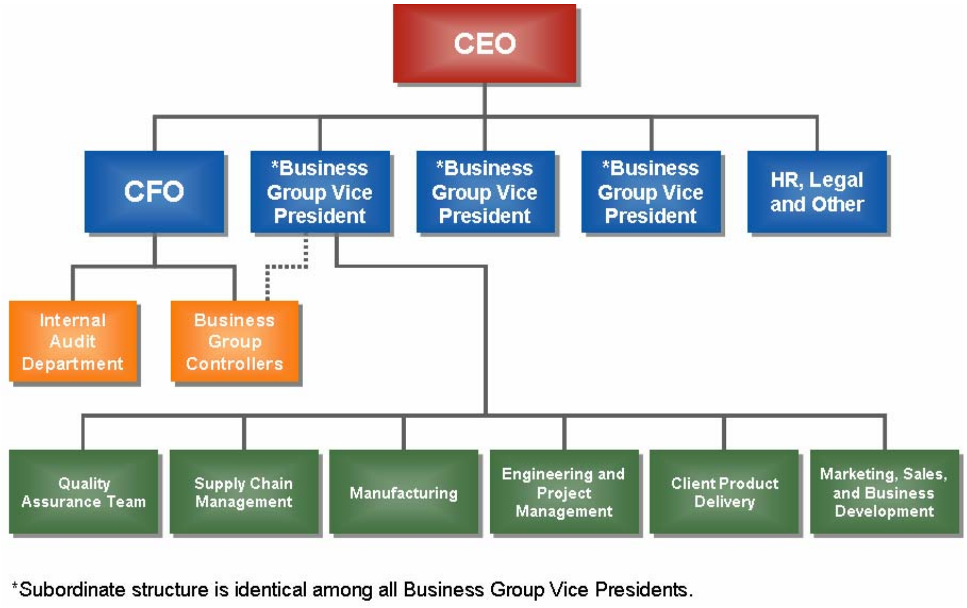
2. As part of global sourcing, many of the organization's customers require product delivery on a just-in-time basis. The organization's strategy is to profitably serve the original-equipment-manufacturer (OEM) and after-market demands for these products. As a result, the organization must carry, or be able to produce, inventory to address the need for a product that may be 40 years old.

3. At one point the organization's board of directors expressed concern about inventory growing faster than revenue — a disturbing trend given that technological advancements could render existing component inventory parts obsolete. The board and management agreed that a focus on production methods and inventory management was an important strategic goal. They recognized, however, that such a focus should not be achieved at the expense of product quality.

Organizational Structure and Goal-Setting

4. The organization is structured around three product business groups. Each of the three product business groups is managed by a Business Group Vice President who reports directly to the Chief Executive Officer (CEO).

5. Product business groups are supported by centralized corporate finance, human resources, internal audit, and other standard back-office functions and have a dotted-line relationship with a product business group controller who is a member of the corporate finance team.


CEO
CFO
*Business Group Vice President
*Business Group Vice President
*Business Group Vice President
HR, Legal and Other
Internal Audit Department
Business Group Controllers
Quality Assurance Team
Supply Chain Management
Manufacturing
Engineering and Project Management
Client Product Delivery
Marketing, Sales, and Business Development

*Subordinate structure is identical among all Business Group Vice Presidents.

6. Each Business Group Vice President is responsible for all aspects of the product business group within the overall corporate strategy, including:

- Marketing, development, and growth of the potential customer base for the product line,
- Oversight of the research and development of requested components for customers,
- Product-line supply chain and supply chain relationship management,
- Product manufacturing process,
- Delivery of manufactured components to customers, and
- Inventory management that supplies high-quality products to customers when needed, yet minimizes on-hand quantities in order to reduce overhead and risk of obsolescence.

7. Components are manufactured to the product-design specifications and quality standards provided by customers, as well as to internal quality standards defined through the organization’s strategic planning process.

8. Each product business group comprises a team of design engineers and process engineers led by an engineering team leader. Each team oversees the design and execution of its manufacturing processes.

9. Executive management develops long-term *strategic focus goals* which are updated every year. These strategic focus goals have been defined by the organization as:

- Focused growth,
- Financial excellence,
- Commercial and technology excellence,
- Process excellence, and
- Outstanding employees.

10. The executive team further develops annual goals and objectives that are linked to the strategic plan. Compensation is based, in part, on the achievement of the specific plans for the business unit. For example, the "commercial and technology excellence" and "process excellence" strategic focus goals include objectives for component product-manufacturing quality, which will be a focal point for this example.

11. Business Group Vice Presidents compare monthly, quarterly, and annual results with the annual strategic goals and report the results to the CEO, CFO, and board. These reports include analysis related to quality, delivery, rework, cost, and overall financial performance.

12. Each product business group employs a quality assurance team that reports directly to the Business Group Vice President. The quality assurance teams are responsible for providing quality monitoring and manufacturing compliance. Business group quality assurance teams often comprise former manufacturing process team leaders, process engineers, and quality assurance professionals with independent quality assurance certifications.

Understanding and Prioritizing Risk

13. Through the goal-setting process, executive management identifies the risks to achieving the organization's goals and objectives, prioritizing them based on their likelihood and significance.

14. The organization has identified a high risk related to the potential failure to manufacture components that meet pre-defined quality standards and the customers' cost requirements. This risk has become more pronounced as the organization seeks to improve production efficiency, reduce finished-goods inventory levels, and continue to meet customer delivery expectations. Thus, the organization seeks to integrate quality considerations into all aspects of the product life cycle — from product design, to manufacturing, to delivery.

15. Internal product-quality expectations are set forth by the CEO and executive management as part of their *commercial and technology excellence* and *process excellence* strategic focus goals. To enhance product quality and efficiency, the organization has implemented a number of lean-manufacturing and quality standards, including the recent adoption of Six Sigma, which Business Group Vice Presidents are required to follow as part of their long-term strategic objectives. Six Sigma — originally developed by Motorola, Inc. — is a set of practices designed to improve processes by eliminating defects. The methodology typically includes the following five steps: define, measure, analyze, improve, and control.

16. During the annual strategic planning process, Business Group Vice Presidents and the leadership teams reporting to them identify and prioritize manufacturing process quality risks. The activity is subjective (i.e., not driven by a quantitative analysis of risk significance and likelihood) and draws on the extensive experience of the people involved. The table below demonstrates the risk assessment thought process and related results.

Product Life Cycle Quality Risks	Risk Cause	Risk Priority
1. Improper design of customer-requested components and related manufacturing processes	a. Inadequate specifications received from customer	M
	b. Failure (through lack of skills or proper design-analysis procedures) to address appropriately the risk that the component will fail	H
	c. Failure (through lack of skills or proper design-analysis procedures) to address appropriately the risk that the component will cause a system failure or not operate as intended in the system in which it is installed	H
	d. Failure to follow established manufacturing design procedures related to: • raw material selection • production methods • testing routines	H
2. Improper manufacture of components within quality tolerances	a. Failure to establish proper quality-tolerance metrics	H
	b. Failure to follow up when tolerances are exceeded	M
	c. Inadequate skills of manufacturing personnel	M
	d. Inadequate oversight of manufacturing process (other than risk 2.b. above)	M

Product Life Cycle Quality Risks	Risk Cause	Risk Priority
3. Untimely delivery of components to customer	a. Failure to establish reasonable delivery deadlines with customer	M
	b. Failure to recognize delays in a timely manner for possible correction or discussion with customer	M

17. This example will expound further on internal control and related monitoring regarding Risk #1 above, *improper design of components and related manufacturing processes.* For simplicity we will refer to this risk as "Design Risk."

Understanding the Internal Control System and Identifying Key Controls

18. Management has implemented the controls in the following table to address Design Risk. Controls with the "🗝" symbol are designated as key controls. Note that the organization does not formally designate controls as "key" or "not key." These controls are designated as key in this example because management has determined that, by monitoring them, it can reasonably conclude whether the internal control system is operating as intended with respect to the identified risk. Note also that the designation as "key" is not necessarily an indication of the control's overall importance to the internal control system. Rather, it is an indication of the relative contribution that monitoring the control will provide to a conclusion about the effectiveness of the internal control system in addressing the related risk. All of the controls below are important, but the effectiveness of some can be determined through the monitoring of others.

Control	Description	Comments
1. Proper skills and oversight	An experienced project manager from the business group engineering team oversees the execution of the component-manufacturing process and leads a manufacturing project team composed of system, design, and manufacturing-process engineers and a representative from the business group quality assurance team.	Management's direct interaction with project team members and their monitoring of the key controls identified below provide the necessary support for a conclusion about the level of skills present and the adequacy of manufacturing oversight.
2. Standard development templates	The project manager uses standardized templates and develops proposed time and resource budgets to track project results against expected outcomes. He or she also coordinates project budgets and costing with the organization's corporate finance team.	Management's monitoring of the key controls below will identify the failure to use standard development templates before such failure would be likely to cause a material error.

Control	Description	Comments
3. Standard contract language	The standard customer contract contains specific language that highlights the requirement for the customer to submit complete and accurate component specifications. The standard contract language serves as a communication mechanism to ensure that the customer understands its responsibilities.	Standard contract language is an important control, but monitoring key control #12 below (the customer's approval) is a better indicator of the customer's understanding and acceptance of its responsibility.
4. Component Design Risk Analysis 🔑	To address the risk that a designed component will not function properly, the manufacturing project team completes a *Component Design Risk Analysis*, identifying and ranking the cause and effect of potential component failures.	These two controls are identified as key because (1) their failure would raise the organization's risk regarding the design of a component to unacceptable levels, and (2) monitoring their effective operation helps support a conclusion about the effectiveness of earlier controls.
5. System Risk Analysis 🔑	To ensure proper operation of the component within the system for which it is intended, members of the manufacturing project team perform a *System Risk Analysis* that identifies and ranks the cause and effect of potential system failures after the component is installed.	
6. Review and approval of component design	Before designing the component-manufacturing process, the manufacturing project team reviews and approves both the *Component Design Risk Analysis* and the *System Risk Analysis*.	This self-review procedure is an important control, but (1) it is not conducted by someone objective enough to provide persuasive support to management levels above the project team, and (2) its failure would most likely be detected (before it could allow a material error) by monitoring key controls #4 and 5 above. As a result, it is not identified as a key control for monitoring purposes.
7. Preparation of Manufacturing Process Flow	The manufacturing project team completes a *Manufacturing Process Flow* to establish the most effective and efficient manufacturing process and to assist in completing the *Manufacturing Process Risk Analysis*.	A failure of this important control would be detected on a timely basis through monitoring of key controls #8, 9, 10 and 12 below. Thus, it is not identified as a key control for monitoring purposes.

Control	Description	Comments
8. Manufacturing Process Risk Analysis 🗝	The manufacturing project team completes a standard *Manufacturing Process Risk Analysis* that identifies and prioritizes potential failures of the manufacturing process.	Similar to key controls #4 and 5 above, these three controls are identified as key because (1) their failure would raise the organization's risk regarding the manufacture of a component to unacceptable levels, and (2) monitoring their effective operation helps support a conclusion about the effectiveness of earlier controls.
9. Manufacturing Process Control Plan 🗝	A *Manufacturing Process Control Plan* (including key sampling metrics, expected manufacturing results, and approved responses to identified results that are outside process expectations) is completed to ensure that design specifications are met during production.	
10. Manufacturing testing process 🗝	Prototypes are manufactured and tested during the development of the *Manufacturing Process Risk Analysis* and the *Manufacturing Process Control Plan.* The manufacturing project team is advised of deviations from expected results outlined in the *Component Design Risk Analysis* and *System Risk Analysis* and updates those analyses appropriately.	
11. Review and approval of manufacturing design	The manufacturing project team reviews and approves the *Manufacturing Process Flow, Manufacturing Process Risk Analysis,* and *Manufacturing Process Control Plan* before design commences of the component manufacturing process.	Consistent with control #6, this self-review procedure is an important control at the manufacturing project team level, but it is not objective enough to be considered a key control at higher levels in the organization.
12. Customer approval 🗝	Before the organization initiates production of the component, formal customer approval is required of the following documentation: - Component Design Risk Analysis, - System Risk Analysis, - Manufacturing Process Risk Analysis, and - Manufacturing Process Control Plan.	This control is designated as key because it completes the communication cycle with the customer and provides independent verification that the customer is satisfied with the component design and manufacturing plan. The failure of this control could increase the organization's risk to unacceptable levels, yet not be detected in a timely manner by other controls.

Identify Persuasive Information about the Execution of Manufacturing Process Quality Controls

19. Because product quality is so important to the organization, management has developed robust ongoing monitoring of quality indicators including:

- The results of the Six Sigma process mentioned above,
- Monthly comparison of quality metrics (described below) across product lines,
- Monthly operating calls, facilitated by the CFO, including Business Group Vice Presidents, and business group controllers to discuss operating results and quality issues, and
- Routine reporting to manufacturing plant leadership, business unit leadership, executive management, and the board of directors of defect and warranty levels.

20. The information used in these ongoing monitoring procedures is indirect. Available indirect information that may indicate a manufacturing-process quality failure includes:

- Number of prototype failures;
- Qualitative prototype failures compared to expectations outlined in the *Component Design Risk Analysis* or *Manufacturing Process Control Plan* (e.g., failures of a type not anticipated in the design phase may indicate improper analysis of the risk of failure);
- Prototype-development scrap levels;
- Extent of revision information noted on the *Component Design Risk Analysis* and *System Risk Analysis*;
- Project time budgets and costs;
- Project status updates from the project manager to the engineering team leader and from the engineering team leader to the Business Group Vice President; and
- Production statistics regarding scrap, rework, and warranty levels.

21. The frequency and level of detail of this indirect information are such that the organization can quickly identify quality problems — however, nearly all of it is produced either late in the component manufacturing development process or after production has already started. Further, some of the information, such as levels of prototype failures, could lead to inaccurate conclusions about control effectiveness. For example, low levels of prototype failures may indicate that both the component and the related manufacturing processes have been designed well,

but such low levels could also result from ineffective prototype-testing procedures. Accordingly, the organization also performs direct monitoring of certain controls in order to gather more timely and reliable information about the operation of underlying controls. The organization has access to the following direct information regarding the operation of controls that address Design Risk:

- Customer's acknowledgement that it provided to the organization complete and accurate component requirements and information (specifications, tolerances, systems in which component will be used, etc.);
- Manufacturing project team's documented acceptance or rejection of the *Component Design Risk Analysis* and the *System Risk Analysis*;
- Manufacturing project team's acceptance or rejection of the proposed *Manufacturing Process Flow*, *Risk Analysis*, and *Manufacturing Process Control Plan*;
- Information obtained during development of the manufacturing project team's proposed manufacturing process per the *Manufacturing Process Control Plan*; and
- Customer's acceptance or rejection of the *Component Design Risk Analysis*, *System Risk Analysis*, *Manufacturing Process Risk Analysis*; and *Manufacturing Process Control Plan*.

Implementation of Component-Manufacturing Project Quality Monitoring

22. The following table highlights how the various levels of management — from the Component Manufacturing Project Manager, to the Business Group Vice President, to the CEO — monitor the effectiveness of an individual component-manufacturing process:

Monitoring Procedure	Information Type	Monitoring Type	Comments
Component-Manufacturing Project Manager			
1. Day-to-day interaction with and oversight of the component design and manufacturing design processes.	Direct	Ongoing	The Project Manager's direct involvement in overseeing every aspect of the manufacturing process and the completion of the self-review procedures gives him or her relevant, reliable, and timely information about whether internal control over Design Risk is operating effectively. This direct interaction can relate to all of the controls identified above, but is especially important with respect to the identified key controls. However, the Project Manager's extensive involvement can also impair objectivity, which affects the ability of others above the project manager level to rely on monitoring at this level.
2. Completion of the self-review procedures described in controls #6 and 11 above.	Direct	Ongoing	

Monitoring Procedure	Information Type	Monitoring Type	Comments
Business Group Vice President			
1. Direct reports from the quality assurance teams. The quality assurance teams review direct information supporting the effective completion of each of the key controls identified above, including the: • Component Design Risk Analysis (Control #4) • System Risk Analysis (Control #5) • Manufacturing Process Risk Analysis (Control #8) • Manufacturing Process Control Plan (Control #9) • Manufacturing testing process (Control #10) • Customer approval (Control #12)	Direct	Ongoing	These quality assurance teams formally report to the Business Group Vice Presidents. While they work closely with the manufacturing project teams, they are objective with respect to the component and manufacturing design processes. Their primary responsibility is to ensure that proper quality procedures are followed. Their close proximity to the operation of the controls, coupled with their objectivity, allows the quality assurance teams to be a primary monitoring mechanism for management.
2. Daily, weekly, monthly, and quarterly review of the indirect information described earlier.	Indirect	Ongoing	As noted earlier, the level of detail provided by this indirect information enables the organization to identify and react quickly to manufacturing quality issues if they arise. Such reactions would typically include correcting the design or manufacturing problem and initiating a separate evaluation of the controls to identify and correct the problem's root cause.

Monitoring Procedure	Information Type	Monitoring Type	Comments
CEO and Executive Management Team			
1. Daily interactions with the three Business Group Vice Presidents in which the results of other quality monitoring procedures are discussed (e.g., quality assurance team results, quality metrics results, financial results, etc.)	Direct and Indirect	Ongoing	Because the organization is highly focused on product quality, daily interactions between executive management and the Business Group Vice Presidents often address quality-related matters. These interactions, although often informal, serve as important support for executive management's conclusions about controls over product quality, including Design Risk.
2. Monthly management meetings in which the results of other quality monitoring procedures are more formally discussed.	Direct and Indirect	Ongoing	These monthly meetings, conducted in the first week of every month, provide a more rigorous analysis of the results of direct monitoring below the executive management level and of the indirect quality metrics.

Identifying Issues and Communicating Results

23. Because the organization's structure is relatively flat, the results of monitoring can be communicated to the proper levels quickly and accurately. Also, because product quality is so important, the communication protocols regarding quality issues are designed to escalate rapidly to the Business Group Vice Presidents, executive management, and the board.

24. The organization does not have a formal control deficiency prioritization protocol, but it does track issue identification and resolution through a "Corrective Action Status" report that is updated continuously and reviewed at the monthly management meeting.

Summary and Observations

25. This manufacturing organization has important quality-related risks that must coexist with often-competing risks associated with financial goals, such as those related to efficiency, on-time delivery, profitability and inventory valuation. Unnecessarily long lead times for finished goods require higher levels of finished goods inventory to meet customer demands, which would negatively affect the

financial goals. Further, a singular focus on production efficiency would likely lead to an unacceptable reduction in product quality.

26. Management and the board have been successful in developing an internal control system and related monitoring that enhance product quality *and* efficiency through a focus on minimizing defects and planning up-front. The controls associated with ensuring that the designed component will work within its intended system, and the controls over the design of the manufacturing process, are also critical to meeting the organization's quality and financial goals.

27. The organization monitors these controls on an ongoing basis through the use of both direct and indirect information. Most of the direct-information monitoring occurs through the normal functioning of the quality assurance teams. These teams, which include highly competent and objective personnel, have direct access to the information required to determine whether these controls are operating effectively. Day-to-day interactions — the effectiveness of which is bolstered by the flat organizational structure and the high-profile nature of the quality-related risks — are also an important form of direct monitoring.

28. The results of the ongoing monitoring are further supported by robust monitoring using indirect information. This indirect information, which includes specific quality metrics as well as financial metrics, enables the organization to identify potential issues that may negatively affect the quality goals, financial goals, or both. This detailed information is reviewed at every level within the organization, including the executive-management level, to ensure that any significant deviations from expectations are identified and explained.

29. The organization makes extensive use of ongoing monitoring procedures because such monitoring enhances their ability to achieve their objectives. Building monitoring into daily operations enables the organization to identify and correct control problems quickly before they can lead to a material failure. As ongoing monitoring identifies problems or potential problems, the organization can employ separate evaluations to further examine and correct them.

Monitoring Certain Information Technology (IT) Controls

1. The earlier examples in this section are based on the internal control systems and experiences of specific organizations. They are designed to demonstrate monitoring by following an identified risk through the sequence of prioritizing the risk, identifying the key controls and persuasive information about those controls, selecting and executing a monitoring procedure, and assessing and reporting the results. Their scope is narrow (concentrating on a *few* risks and controls) in order to focus on each step in the monitoring process.

2. The examples in this section on Monitoring Certain Information Technology (IT) Controls differ slightly from the others in that they explore several common IT-related risks associated with financial reporting and the monitoring of internal controls related to those risks. It considers the types of controls used to mitigate common risks, discussing the types of information used to verify that those controls are operating. It also provides examples of common IT management processes that, in the right circumstances, might be considered to be control monitoring activities and also examines how technology tools can be used to monitor certain controls. Note that, while the focus of this example is on financial reporting objectives, the concepts can be applied to operations-related objectives or to compliance with laws and regulations.

Understanding and Prioritizing Risk

3. Although IT-related risks are applicable to nearly every organization, the prioritization of those risks and the relative importance of different types of controls that mitigate them will vary from organization to organization. The table below summarizes some of the most common IT-related risks associated with financial reporting and contains summary examples of factors that can be considered in determining the relative importance of the given risk.

Nature of Risk[6]	Risk Description
1. Inappropriate Access	Application programs are accessed and used inappropriately, resulting in errors, invalid transactions, or fraud.

[6] The terms in the Nature of Risk column in this table serve only to provide a brief name to each risk that will facilitate linkage throughout the remainder of the discussion. Readers may note that the names do not capture completely the essence of the related risk.

<table>
<tr><th>Nature of Risk[6]</th><th>Risk Description</th></tr>
<tr><td colspan="2">Example Factors Influencing Risk Prioritization:
• Degree to which inappropriate access might benefit someone who obtains it — For example, system access that might allow someone to steal money, manipulate transactions for personal benefit, or conceal illegal activity is a greater risk than system access that offers little or no benefit to inappropriate access.
• The significance of the data processed by the system and its potential to affect organizational objectives in a material manner</td></tr>
<tr><td>2. Program Integrity</td><td>Application program processing logic (source code, configuration information, etc.) is subjected to unauthorized or improper setup or modification, rendering the system incompatible with user needs or expectations and causing incomplete or inaccurate information processing or reporting.</td></tr>
<tr><td colspan="2">Example Factors Influencing Risk Prioritization:
• Packaged versus internally developed application systems — Relative to <i>programming logic</i>, packaged application systems typically carry less risk than internally developed systems because packaged application systems offer limited or no access to the source code. However, because they are created to be used by a wide variety of organizations and typically include more configuration options than internally developed systems, packaged application programs can carry a higher level of risk regarding the selection of options and the resulting integrity of the <i>configuration information</i> that controls how programs function.
• Programming complexity — Application programs that perform complex calculations or controls (sophisticated financial computations, pricing discounts, etc.) — where end users are less able to confirm complete or accurate processing — typically are higher-risk than applications that merely accumulate and aggregate business transactions. For example, a bank's program integrity risk profile related to loan and deposit applications might be considered "high" due to the nature of processing a large volume of transactions having a vast array of calculations across different product types. By comparison, a manufacturer's customer-invoice computations may be less complex and easily verifiable to specific customer orders and physical shipment records.
• The significance of the data processed by the system and its potential to affect organizational objectives in a material manner</td></tr>
<tr><td>3. Data Integrity</td><td>Data is improperly added or altered, and could include business transaction data (e.g., an invoice), master file data (e.g., a customer credit limit), or parameter settings that control processing logic or enable controls (e.g., a system setting that triggers an additional level of approval over a certain dollar limit).</td></tr>
<tr><td colspan="2">Example Factors Influencing Risk Prioritization:
• Degree of complexity associated with data entry — Data integrity risk is greater in systems requiring complex and/or multi-step data entry than in systems with simple data entry procedures.
• The significance of the data processed by the system and its potential to affect organizational objectives in a material manner</td></tr>
</table>

<table>
<tr><th>Nature of Risk[6]</th><th>Risk Description</th></tr>
<tr><td>4. Information Processing</td><td>Processing fails or is erroneous, resulting in incomplete, inaccurate, or lost data.</td></tr>
<tr><td colspan="2">Example Factors Influencing Risk Prioritization:
• Extent of information interchange — Information processing risk is commensurate with the number of internal and third-party data interfaces.
• Potential for system outage or failure that results in disrupted or impaired information processing
• The significance of the data processed by the system and its potential to affect organizational objectives in a material manner</td></tr>
</table>

Identifying Key Controls and Information Used to Monitor Those Controls

4. The specific types and placement of IT controls to address prioritized risks can also vary considerably. The size and sophistication of an organization, the number, nature and location of its underlying technology resources, its organizational structure, and its IT-development philosophy can all affect the nature of the specific controls in place for managing IT risks. Variations in these factors affect the relative importance of specific IT controls which, in turn, may drive different types of monitoring processes. In addition, at times monitoring manual controls can provide sufficient support for a conclusion regarding the effectiveness of IT controls that operate earlier in the transaction process. For example, in a small organization the Chief Financial Officer (CFO) may sign every check after reviewing supporting invoices. This control, if it operates effectively, enables the CFO to identify unauthorized checks generated by someone with improper system access. It can also serve as a compensating control where segregation of duties between check writing and cash accounting is not practical.

5. Although specific controls and related monitoring processes can vary, the following table summarizes IT controls that generally are important in mitigating one or more of the broad risks defined earlier. This table also links to the types of risk that the controls address (see Nature of Risks above) and provides a high-level view of the direct information typically used to monitor whether these controls are operating.

IT Control Type	Risk(s) Addressed	Control Description	Information Used in Monitoring
Limited Access to Application Program Source Code	• Inappropriate Access • Program Integrity	Access controls that limit to specific personnel the ability to make application programming and/or configuration changes: - trained in programming tools, and - authorized to make programming changes	• Listing of access rights to source code libraries • Evidence of appropriate access rights approval • Security logs indicating who has accessed a given program
Application Security	• Inappropriate Access	Application access controls that: - provide a restrictive set of access rights to program users based on their responsibility, and/or - provide a foundation for segregation of duties within or between application programs	• Listing of access rights to application programs and/or specific transactions within those programs • Evidence of appropriate access rights approval • Security logs indicating who has accessed a given application
Data Security & Change Control	• Inappropriate Access • Data Integrity • Program Integrity	Access controls that restrict to (a) business users of authorized application programs, or (b) a limited group of data administrators the ability to add or alter financial reporting data Approval controls that provide visibility to and approval of data and database changes made by data administrators	• Listing of access rights to relevant data files, databases, or tables within a database • Evidence of appropriate access rights approval • Evidence of appropriate configuration of master database rules, including application program access rights • Security logs indicating who has accessed a given application or database • Evidence of the identification and transparency/approval of data changes on an exception basis (i.e., changes made through any means other than normal business processes and application programs that require certain levels of approval)

IT Control Type	Risk(s) Addressed	Control Description	Information Used in Monitoring
Limited Access to Production	• Program Integrity • Data Integrity	Access controls and operating system security configurations that restrict to a limited and defined group of personnel the access to operating system administration capabilities (i.e., restrictions to the ability to "push" program changes into the production environment).	• Listing of access rights to relevant production program libraries, files, and related configuration information • Evidence of appropriate access rights approval • Security logs indicating who has accessed a given program
Program Testing	• Program Integrity	Controls designed to ensure that application program changes are sufficiently tested prior to their introduction into a production environment	• Documentation of proper testing of program changes, including those to configuration data. • Documentation of business unit or user approval of relevant changes
Program Change Control	• Program Integrity	Access and approval controls that, collectively, ensure the visibility and approval of application program and/or configuration changes	• Listing of program changes made, indicating source and approval • Documentation of appropriate testing and approval of program and configuration changes before they are moved into a production environment • Evidence of appropriate access rights approval enabling an individual to move programs to a production environment
Job Scheduling & Management	• Information Processing	Access and approval controls over the scheduling and management of the "jobs" (meaning batch jobs and other operational processes originated within IT that are relevant to information processing or protection) that enable complete and accurate processing of data and information	• Listing of access rights to relevant job scheduling and management tools • Evidence of appropriate access rights approval • Evidence that relevant and important "jobs" and other activities are completed as planned (including correcting and resubmitting failed "jobs")

IT Control Type	Risk(s) Addressed	Control Description	Information Used in Monitoring
Data Redundancy	• Data Integrity • Information Processing	Technology and processing controls, including data mirroring and disk or tape backups, designed to ensure that data is not lost due to operational or processing failures	• Reports from backup tools, confirming that all relevant data files and programs are backed up • Comparisons of mirrored data, showing equivalence thereof (usually performed automatically as part of the system's mirroring process) • Results of periodic data recovery tests

Implementation of IT Controls Monitoring

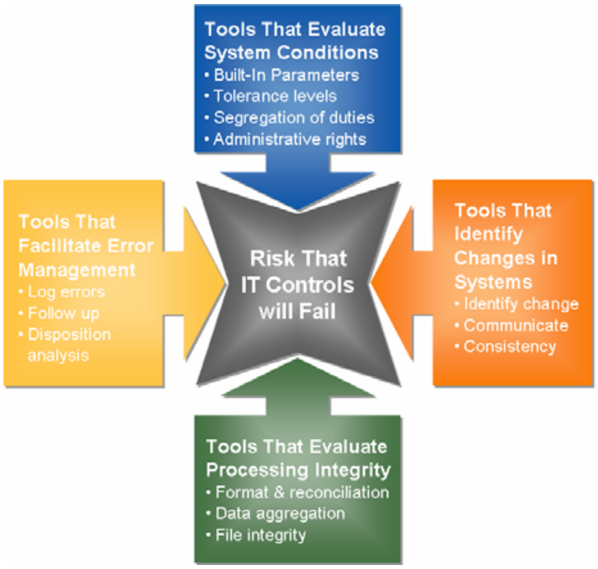
6. IT controls typically are monitored through a combination of ongoing monitoring and separate evaluations. Many IT departments have specific processes in place that, as an output from those processes, can provide management with information about the effectiveness of certain controls. To the extent that those processes work effectively, management may be able to reduce or streamline the monitoring work performed through separate evaluations. Some of these processes provide "direct" information about control effectiveness; others provide only "indirect" information at a much higher level or on a composite (rather than specific-control) basis.

Monitoring Procedure	Information Type	Controls Addressed
Access Recertification	Direct	• Limited Access to Application Program Source Code • Application Security • Data Security & Change Control • Limited Access to Production • Job Scheduling & Management
Description: Security access recertification is a process through which, at a given point in time, the existing access rights to an IT resource (e.g., an application program or an infrastructure component) are provided to the person responsible for that resource. The responsible party compares the existing access information to his or her expectations and identifies potential exceptions, which are investigated and addressed, as required. Because this process occurs outside the normal process for adding and changing user access rights, it can serve as a method of monitoring the effectiveness of the security administration process (whereby		

Monitoring Procedure	Information Type	Controls Addressed
user access rights are added, changed or removed). To qualify as an effective monitoring procedure, exceptions should be analyzed to determine why the security administration process allowed them to occur.		
Security Log Monitoring	Indirect	• Limited Access to Application Program Source Code • Application Security • Data Security & Change Control • Limited Access to Production • Job Scheduling & Management
Description: A common control in any IT environment is the process of "signing on" to an IT resource using some combination of user ID and password or an equivalent. Many organizations log this activity to provide an audit trail of IT resource users. 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 any unusual activity is occurring. For example, this type of analysis might identify impersonation attempts wherein someone with access to another person's user ID tries to guess that person's password. Such activity would be logged as the same user ID making multiple invalid password-access attempts. This analysis provides only indirect information about the effectiveness of the internal controls since the information that is being monitored represents an analysis of failures to gain access to information resources.		
Independent Quality Assurance or Peer Review Over Program Development	Direct	• Program Testing • Program Change Control
Description: In many larger IT environments, an independent quality assurance function (or a peer review process) may review 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.		
Change Review Board	Direct and Indirect	• Program Testing • Program Change Control
Description: Some organizations with frequent and potentially disruptive changes to the IT environment have implemented a "change review board" that provides oversight to the change process. Typically comprising cross-functional IT (and, possibly, business unit) managers — and less formal than the Independent Quality Assurance or Peer Review discussed above — a change review board determines whether all requirements were met (approvals, testing, communication, etc.) before the changes were approved for movement or production, then, collectively, reviews and approves all changes. Whether this activity provides direct or indirect information about the effectiveness of controls depends on the		

Monitoring Procedure	Information Type	Controls Addressed
nature of the information gathered and analyzed during the change review process.		
Post-Implementation Reviews of Program Changes	Indirect	• Program Testing • Program Change Control
Description: Similar to the independent quality assurance processes discussed above, to the extent that an organization 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 typically is performed after a program has been placed into production and is being used in the business. The most effective post-implementation review processes include an evaluation of both the functionality and usefulness of the program and the effectiveness of the internal controls that are built into the application programs and business or accounting processes.		
Recovery Testing	Direct	• Data Redundancy
Description: IT management may perform different levels of recovery-capability testing for different forms of disruption or disaster. To the extent that this testing involves the re-establishment of IT systems using either backup tapes or redundant/mirrored systems, it provides management with direct information regarding the effectiveness of the redundancy or backup controls.		

7. Many organizations use automated tools to monitor the continued effectiveness of certain IT-based controls. The general nature of tools is discussed in the Using Technology for Effective Monitoring section of Volume II. The examples below are specific to IT controls and generally fall into one of four main categories (see Figure 1).


Tools That Evaluate System Conditions
• Built-In Parameters
• Tolerance levels
• Segregation of duties
• Administrative rights
Tools That Facilitate Error Management
• Log errors
• Follow up
• Disposition analysis
Risk That IT Controls will Fail
Tools That Identify Changes in Systems
• Identify change
• Communicate
• Consistency
Tools That Evaluate Processing Integrity
• Format & reconciliation
• Data aggregation
• File integrity

Monitoring Tools
Figure 1

Tools that Evaluate System Conditions

8. Many “controls” that are built into application programs and infrastructure resources are enabled by configuring specific parameters or defining a set of rules. This category of automated tools monitors the consistency of those controls by examining the parameters or rules at a given point in time, then comparing the resulting data to baseline data, a prior analysis, or both to determine their consistency with the organization’s internal control requirements. Often these tools are used to monitor controls in the following ways:

- *Comparing system parameters to pre-established requirements* — Certain security controls and policies are enabled through parameter settings in the base operating system, a database environment, or the configuration of an application program. For example, controls such as the length and complexity of passwords and the frequency with which they must be changed are enabled by security parameters. Tools can be used to scan these settings and compare them to the resources’ internal security policies and internal control requirements.

- *Comparing system results to pre-established tolerance levels* — Certain controls within application programs 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 inventory system uses LIFO or FIFO is dependent on the parameters that define the application configuration. Similarly, the tolerance levels for matching processes (e.g., vendor invoice quantities to a receiving report) are dependent on application configuration. Tools can provide for periodic or continuous visibility of system configuration settings for identifying and evaluating out-of-tolerance settings.

- *Evaluating system access rights for possible segregation-of-duties issues* — Within ERP systems, the ability to limit access rights and segregate incompatible duties is enabled by application security rules that are based on an organization’s definition of roles and the access rights associated with those roles. For example, incompatible duties within or between application programs are identified by comparing existing user access rights to a baseline set of incompatible rights either within a single application or across multiple applications. Tools enhance the effectiveness and efficiency of this potentially complex, time-consuming task.

- *Evaluating propriety of administrator rights access* — In any technology environment, “administrator rights” must be assigned to those responsible for administering the resource(s). Since someone with administrator rights to a resource can perform any function with respect to that resource, most organizations limit these rights to a small group of personnel. Tools can provide management with the information it needs to monitor the assignment of administrator access rights.

9. Tools that monitor information system conditions increase the speed and effectiveness of monitoring, allowing it to be performed on a more frequent basis. Such tools may operate periodically (often described as “scanning based”), or they can operate continuously as an integrated component of software or hardware (often described as “agent based”). The decision as to which approach is correct is driven by many factors, including the:

- Importance of the control,
- Prioritization of the risk it is designed to mitigate, and
- Effort and/or cost associated with using the tool.

Tools that Identify Changes in Systems

10. Tools that identify changes are an extension of those that focus on conditions. The basic difference is that change-identification tools are designed specifically to identify and report changes to critical programs, infrastructure resources, databases, or data so that someone can verify the appropriateness and authorization of those changes. They usually operate continuously to identify relevant changes or, much like tools that focus on business transactions, they analyze log information created by different IT resources, thus highlighting relevant change-related activity that may be significant.

11. Where controlling change is important, organizations typically employ a form of “change control” that includes both a preventive control (e.g., limits to specific personnel the ability to make changes) and a detective control (e.g., all changes are recorded, reviewed, and approved by someone who is independent of those making the changes). Thus, the following considerations should be taken into account:

- Not all IT resources are capable of recording changes;
- In large IT environments, individual resource components may be so numerous that analyzing them on a detective basis would be overwhelming;
- The effects on system performance of some resources’ built-in logging capabilities may be unacceptable; and
- The built-in logging features of some systems are easily disabled, making them unsuitable for use in higher-risk areas.

12. Tools in this category can be used as part of a control activity, part of monitoring activities, or both. For example, if an evaluator uses the information from a tool to identify a change for the purpose of independently verifying that the change was approved, it is likely a monitoring activity. In contrast, if a user employs that same information to investigate and seek approval for the change, it is likely being used as a control activity. If both users and evaluators use the information, the tool serves dual purposes. Specifically, tools in this category can:

- Identify changes that have been made to application programs, database structures or data, and security rights and permissions. These tools can provide visibility to change-related activity so that the activity can be validated independently, thus establishing whether the underlying change-control process works as designed.
- Alert appropriate personnel when certain types of "mission-critical" changes are being made, ensuring transparency throughout the organization and timely action, as necessary. For example, the tools may identify when someone with "administrator" rights makes particular changes or performs certain actions, thus facilitating an independent review of the activity.
- Evaluate whether all planned changes were made consistently and completely. For example, in a certain distributed, integrated, and high-volume transaction system, application program consistency between locations can be part of the controls over the system as a whole. Such consistency may depend on all remote locations' running an identical version of the application program.

Tools that Evaluate Processing Integrity

13. These automated tools are designed to verify and monitor the completeness and accuracy of the various steps that might occur in high-volume and complex application program process streams. For example, multi-site retailers with distributed point-of-sale (POS) systems at stores often employ daily — or even more frequent — processes for transmitting POS data from each store to a central processing environment. Usually, these tools balance and control data as it progresses through processes and systems. Tools in this category can perform activities such as:

- Independently verifying the format and content of data to be processed, avoiding the processing of bad data;
- 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 and operating systems (for example, these tools might be used to ensure the completeness and accuracy of data from

source systems to the general ledger and from the general ledger to data warehouses); and

- Confirming data file, record, and field accuracy as data is aggregated or disaggregated and as it moves across systems and processes.

Tools that Facilitate Error Management

14. Most application programs that interface with other systems are designed with logic that detects transactions that do not meet defined criteria. When such transactions are detected, they often are captured in a suspense area and are investigated and corrected before transaction processing can be completed. 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 that requires investigation and correction before being processed further;
- A telecommunications provider may receive message information from its telephone switching systems regarding customer phone usage, but the customer may not yet have been added to the billing system so that those messages could be rated and billed; or
- A bank may receive properly directed deposit or checking activity, but the customer account number may be invalid.

15. Although these types of systems operate as control activities, monitoring the volume and resolving the activity in these suspense areas substantiate the effective operation of controls over related error resolution. In addition, these tools typically document error resolution, providing an audit trail that provides evidence of control operation.

Assessing and Reporting Results

16. Reporting the results from monitoring controls that address IT risks is the same as for other controls. However, assessing the impact of identified deficiencies can be complicated by the fact that, while many of the IT controls can be pervasive, compensating controls that mitigate deficiencies may also exist in business and accounting processes. Accordingly, effective communication between IT and accounting and financial reporting is essential to efficient and effective assessment of the results of the monitoring process.

17. Some organizations also have IT "problem management" processes. Problem management differs from, but is related to, incident management. The purpose of incident management is to return IT applications and services to normal levels as soon as possible and with the least possible business impact. The principal

purpose of problem management is to find and resolve the root cause of a problem, thereby reducing future incidents.

Summary and Observations

18. Nearly every organization has information technology risks that are meaningful to organizational objectives. However, those risks may be prioritized differently across different systems and organizations. The risk factors discussed above are intended to help organizations customize their IT risk prioritization efforts.

19. Once risks are prioritized, organizations can focus monitoring efforts on the controls that are most important in managing or mitigating those risks — noting that the controls may reside outside of the IT environment (e.g., the CEO's manual check-signing or other manual controls that, on a timely basis, confirm the validity of information processing).

Appendices

The following appendices include excerpts from actual company documents that relate to one or more of the examples presented in this Application Techniques volume. Organization names have been removed and other potentially identifying features, such as department names and report titles, have been altered to preserve the privacy of these organizations.

ABC Company COSO Usage Document

Related to Example 1

Notes about the material

This document contains excerpts from a longer, 30-page document prepared by a large professional services organization (ABC Company). The organization updates the document annually and uses it to facilitate and communicate responsibilities and expectations about how the organization achieves the principles contained in the COSO Framework. The excerpts included here are related specifically to how the organization addresses the risk assessment and monitoring components of internal control.

Table of Contents

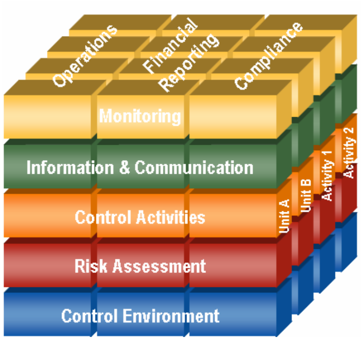
Overview

Implementation of the COSO Framework

1. ABC Company has selected the Committee of Sponsoring Organizations (COSO) framework as the guiding framework for internal controls over financial reporting. In relation to the Financial Reporting section of the framework, the framework's general objectives and guidelines have been mapped to ABC Company's processes and activities; thus execution of the objectives in the framework should occur naturally as part of ABC Company's normal activities.

2. The COSO framework includes a number of specific activities that support and reinforce each other. As a set of general principles:

- Control Environment activities set the "tone from the top", are widely spread and set the appropriate tone for the organization. These activities are generally monitored and/or tested on an annual basis to demonstrate good enterprise-wide awareness and compliance.



- Widely spread control activities that are related directly to financial integrity and/or fraud prevention are noted as part of the Control Activities and are tested on a regular basis.
- Closely held activities which do not require the same level of widespread execution are listed in Monitoring, Risk Assessment or Information & Communication. Some of these activities are included in the control activities (and, thus, are widely tested), but the majority of them are simply outlined and confirmed as executed on an annual basis.

3. Each section of the COSO framework is summarized, and the key ABC Company activities are outlined after the COSO framework summary.[7]

[7] To conserve space, and to remain focused on the monitoring component, only the Risk Assessment and Monitoring sections of ABC Company's *COSO Usage Document* are included in this appendix. Risk Assessment is included due to its direct effect on ABC Company's monitoring.

Risk Assessment

4. In the COSO definition, Risk Assessment recognizes that for an entity to exercise effective controls, it must establish objectives and understand the risks it faces in achieving those objectives. Management should understand the implications of relevant risks that might hinder progress toward its objectives, and then management should provide a basis for managing those risks.

5. At the summary level, the COSO framework outlines several areas of focus that should be considered in order to establish an effective Risk Assessment process.

Area of Focus	ABC Company Expectations
Entity-Wide Objectives	• Broad statements of what an entity desires to achieve, supported by strategic plans. • Effective Communication of those objectives (to board and employees). • Consistency of Strategy and Objectives. • Consistency of business plans & budgets with entity wide objectives, strategic plans, and current conditions.
Activity (Unit) Level Objectives	• Activity (unit) level objectives should link to entity-wide objectives and strategic plans. • Activity level objectives should be consistent and complementary. • Objectives are established for each significant business process area (where relevant). • Adequate resources exist to achieve objectives. • Prioritization of objectives to ensure achievement of entity objectives. • Involvement in all levels of management in objective setting, to ensure commitment to objectives.
Risks	• Consideration of external and internal factors that could impact achievement of objectives (with risk analysis, to provide management a basis for managing the risks). • Adequate mechanisms to identify risks externally and internally. • Identification of risks for each activity (unit) objective(s). • Thoroughness and relevance of the risk analysis process (formality of the process, involvement of Sr. Management, etc.).

Area of Focus	ABC Company Expectations
Managing Change	• Mechanisms must exist to identify and react to routine events or activities that could effect achievement of objectives. • Mechanisms to identify dramatic or pervasive shifts — such as programs to identify customer demographic or paradigm shifts, workforce skill shifts, etc. • Introduction of new personnel is appropriately managed to introduce them to the organization’s culture & ensure awareness of their controls. • New Information Systems are adequately assessed for impact, to ensure controls are adequate, to ensure system was appropriately developed, and properly implemented (processes designed, employees trained, etc.). • Rapid growth is managed via supporting systems capability growth; supporting workforce additions as needed to support the growth (ex: accounting staff), budgets are revised appropriately, and interdepartmental issues caused by plan revisions are addressed. • New Technology developments are monitored (information is gathered; competitors use is considered, mechanisms exist to introduce new technology into the organization). • New Products are reasonably forecast; IT and staffing is sufficient; early results are tracked; impact on other company products is evaluated; overhead is evaluated to reflect product contribution accurately. • Restructuring or Downsizing is planned in such a way that reductions are analyzed for impact on operations, terminated employees control responsibilities are reassigned, impact on morale is considered, and safeguards exist to protect against disgruntled employees. • Foreign Operations are evaluated regularly; management is aware of political, regulatory, etc. issues; personnel are aware of accepted customs and rules; procedures exist in case communications are interrupted.

Risk Assessment & Risk Management Activities

6. While utilizing other frameworks to manage overall risk, ABC Company includes a set of activities that align with the first three areas of focus; occurring at the company-wide (or entity) level, the deployed entity level, and the project level. Change management activities are summarized at the end of the section.

Entity & Unit Level Objective Setting

7. Entity and activity objectives are established and communicated through the planning process:

- The planning process is anchored by a 5 year strategic plan, which is updated annually. The 5 year plan encapsulates our strategic intent in a series of strategies with respect to type of work mix (revenue growth by service group), target margin structures by service group, workforce evolution to support target work mix, SG&A targets, SE pyramids headcount, and units and financial strategy (sources and uses of cash, equity programs).

- The five-year plan is then used as a key input into the next fiscal year annual plan (along with current operating data), which drives the entities key financial objectives into each organizational unit (P&L and cost center). The annual plan is an integrated plan; all major entities are included and plan results aligned to overall entity results.
- Each entity then completes a detailed plan, with consideration of a variety of factors (market conditions, etc.), and the opportunity to adjust the top level plan as detailed plans are completed. Plans are completed at the lowest P&L or significant cost center level, and approved by the leader of that unit, and reviewed by management as needed.
- During the fiscal year, each organizational unit completes a quarterly forecast. Once completed, the plan is updated on a quarterly basis through the quarterly forecasting process; adjustments in operations (such as reductions or increases in hiring, etc.) are identified and communicated as required to achieve the plan across entities. Each entity is then responsible for operationalizing specific changes (such as cost reductions, etc.) required to achieve the corporate objectives. The forecasting process also provides opportunities to request additional funding and modify budgets as appropriate (based on reviews).
- Achievement of objectives is monitored through a variety of reporting packages; a common core set of reports are produced by SAP with a common core set of metrics. Metrics vary logically between P&L and cost center units.

8. Once completed, a summary of the plan is communicated in a variety of ways, including (but not limited or exclusive to):

- The Board of Directors reviews and approves a summary of the financial plan.
- Senior Executives are given a copy of the ABC Company Business Plan, which includes an overview of the company’s financial and operational priorities for the year.
- Most personnel have the opportunity to attend communication events to learn about the organization’s focus. These generally occur via webcast, or possibly via community meetings. (Exceptions relate to technology access and some specific business situations)

9. In addition to the planning process outlined above, a number of detailed (but relevant) activities occur to monitor risks and drive strategic objectives through the organization. Specifically:

- The ABC Company Growth & Strategy team completes a number of strategic assessments which address various strategic and operational issues (for example, analysis of margin results) or external issues. The efforts of the Growth & Strategy team are under the direction of the Executive Leadership team, reporting directly to the Chief Strategy and Corporate Development Officer (by role, title may vary), to ensure appropriate visibility to the "road signs" of change.
- On a periodic basis, as determined primarily by the Chief Executive Officer, ABC Company may undertake a large-scale, comprehensive review of our strategy which would include an examination of internal (e.g., ABC Company recent performance) and external (e.g., competitive environment, market trends) which inform the refinement of our strategy. This process also includes an analysis of various risks including market and competitors.
- ABC Company maintains an Office of Government Relations team and Global Asset Protection team that monitor political trends. As with the Growth & Strategy team, specific issues are identified and acted upon based on the political risk to the organization. Briefings are provided to ABC Company leadership on an as needed basis.
- ABC Company completes an annual risk assessment, which is a cross functional, external and internal risk assessment. A number of different risk areas are evaluated (for impact and increasing/decreasing risk), and Senior Management uses this data as an input into the planning process. The process reports to the Chief Risk Officer, and is driven by Internal Audit; results are shared with senior leadership.
- ABC Company's Office of the CEO maintains an organization Operating Model that establishes how the company operates, how the company is organized and how the various entities and roles in the organization work together to provide effective and efficient customer service. This document is updated throughout the annual cycle to reflect any changes in the organization and serves as one of many management tools to execute the strategic plan and objectives that are developed.
- Programs are created to address specific risks, or drive specific objectives across units. Program execution is monitored by the Growth & Strategy team, reporting to the COO.

- Regular Management meetings occur at all levels to monitor risks, address issues and prioritize activities and objectives, and to monitor progress in achieving objectives (P&L level, Cost Center level, Corporate Level).
- Specific activities occur in each node to monitor specific risks. As an example, HR monitors attrition; CIO monitors application backup activities. Specific to IT, strategic technology trends are considered on a regular basis as a part of the IT Strategy; this is outlined in more detail in the IT Body of Evidence document.
- Benchmarking of major functional areas (Cost of Finance, Cost of CIO, HR service at a macro level, etc.) occurs to ensure competitive and reasonable results across the organization.

Contract Level Risk Assessment and Management Activities

10. The heart of ABC Company's business is contracts. Accordingly, a set of Risk Assessment and Management activities exist to ensure that contract risks are appropriately identified, considered, and managed:

- Each P&L unit considers the appropriate customers to pursue as a part of their annual planning exercise (including the consideration of risk to the unit and to ABC Company), resulting in a target set of customers. Although the target set of customers is not exclusive, the majority of Sales & Marketing efforts are directed at these customers.
- All contracts go through an approval process at a variety of levels in the Operating Group, which considers the risk inherent in the contract (and balances the return on the contract with the risk)
- All large and complex contracts meeting a specific set of criteria go through a special approval process via the Capital Committee, which is chaired by the Chief Risk Officer. This process ensures that senior leadership has the opportunity to consider the risks on these large contracts. The Capital Committee's process includes reviews by a number of subject matter experts (Legal, etc.) and an explicit, standardized risk management assessment.
- In accordance with the Quality Assurance (QA) process, a QA review is required for all opportunities during the selling phase prior to submission to the customer for all new opportunities. The frequency and timing of opportunity QA reviews vary based on the size and risk of the opportunity — larger/riskier opportunities are subject to more frequent QA reviews. QA reviews are required for all contracts during the delivery phase. The frequency and timing of delivery QA reviews are to be aligned

with key project milestones; however, the highest risk projects must have QA reviews at least quarterly.

- ABC Company methods are employed to reduce risk by providing contracts with a standard methodology to follow in executing the contract. Methods are updated on a regular basis to recognize changing market dynamics and new research.
- Customer satisfaction is monitored on an ongoing basis, via web-based surveys. This allows customers an independent method of raising issues across the work being performed for a customer. Across customers, ABC Company management monitors results for market trends and issues.

Corporate Contract Risk Monitoring

11. At the corporate level, a number of activities occur to monitor risk:

- High Risk contracts are monitored for risks that would harm the entity. Contracts with a specific risk profile are identified and escalated through the "High Impact" reporting process. As contracts' risk profile increases, management attention escalates, to ensure the appropriate amount of monitoring & intervention is occurring.

Other Risk Monitoring Activities

12. A variety of other activities occur to monitor risk; the most notable of these include crisis monitoring & response:

- ABC Company's Global Asset Protection Team monitors news and security sources for geopolitical issues or natural disasters that impact our operations worldwide. As situations warrant, the team contacts or is contacted by local management. The team has an escalation path to a corporate Situation Management Committee, which includes appropriate (based on situation) senior leadership.

Risk Monitoring Summary

13. At the summary level, the following chart illustrates how ABC Company's activities support the Risk Assessment area of the COSO framework. This is an illustrative chart only; the detail above is intended to represent the actual activities.

Activity	Responsible	Entity Objectives	Activity (Unit) Objectives	Risks
Annual Risk Assessment	Chief Risk Officer	✓		✓
5 year Strategic Plan, updated min 1x per year	Chief Strategy and Corporate Development Officer	✓		
Annual Plan, driven to P&L/Cost Center Level	Finance Operations	✓	✓	
Quarterly Forecast, tied to corporate objectives	Finance Operations		✓	
Customers are targeted, including assessment of aggregate risk	Operating Group COO		✓	✓
Contracts are reviewed and approved, including risk assessment	Operating Group	✓	✓	✓
Large & Complex Contracts meeting guidelines go through a separate review process via Capital Committee	Capital Committee	✓	✓	✓
Contracts go through quality reviews	Chief Risk Officer/ OG COO			✓
Customer Satisfaction is monitored on a regular basis	Chief Risk Officer/ OG COO			✓
Key customer financial situation is monitored	CFO			✓
High Risk Contracts with potential issues are monitored by various levels of Senior Management	Chief Risk Officer	✓		✓
Geo Political Monitoring	Growth & Strategy, Office of Gov't Relations; Asset Protection			✓
Periodic ethics and compliance risk assessment	Compliance Officer			✓

ABC Company Change Management Activities

14. The COSO framework notes that effective change management is an important part of risk assessment, and ABC Company completes a number of different activities to monitor and address events that could disrupt operations.

Management of these change events — at the ABC Company or entity level — is distributed across a number of different groups, as outlined below.

COSO Change Management Area	Responsible	ABC Company Activity
Anticipation of Internal & External events that could impact ABC Company	Office of Gov't Relations, Growth & Strategy; Internal Audit; Global Asset Protection	• Externally, as noted above, risk assessment activities include monitoring of key external trends and monitoring of political risks that could disrupt the entity.
	Growth & Strategy	• Internally, the Growth & Strategy team provides a tracking for major internal programs (combined with selected external trends) to provide Sr. management with ability to influence major changes in the organization.
	Business Architecture	• In addition, Business Architecture/Operational Programs tracks major internal operational programs outside of the strategic programs tracked by Growth and Strategy.
Changed Operating Environment — Changes in the operating environment that could impact ABC Company	Growth & Strategy Internal Audit	• As noted earlier, Growth & Strategy & Internal Audits both assess external trends that would create risk for the entity (such as declining margins, etc.).
	Legal	• Legal monitors selected elements of the regulatory environment for changes that would create risk for the entity, and provides updates to management on key trends.
	Growth & Strategy; HR	• External labor market trends are monitored primarily by HR with some work by G&S; internal employee trends are monitored via Global Employee Surveys. Employee engagement is explicitly included and monitored as a part of corporate metrics.
	Operating Groups/Growth Platforms	• OG Resource planning process considers inputs from a variety of sources to balance resource needs and regularly (quarterly) revise the staffing & recruiting needs as a part of the quarterly forecasting process.

COSO Change Management Area	Responsible	ABC Company Activity
New Personnel — Certainty that personnel are aware of ethical standards; controls continue to execute	HR/Ethics and Compliance Office	• New personnel go through an orientation process that touches on key aspects of ABC Company's culture, including the Code of Business Ethics and related policies, and as appropriate, execute training on Internal Controls over Finance Reporting as well as operational controls related to other processes, if relevant. Also includes specific Corporate Required Training based on level and function.
	HR	• Control responsibilities (macro level) have been added when relevant to position responsibilities to ensure the responsibilities are kept independent from the incumbent and remain intact as people change jobs.
	Business Leads	• Business Leads and Local Control Leads are responsible for communicating and monitoring assignment of controls to ensure execution responsibilities are clear.
New Information Systems consider controls; are properly developed, and the impact on the organization when the go live is assessed	CIO	• IT controls include controls related to the System Development Lifecycle, including the appropriate development, testing, and installation controls. • System development projects include a communication or change management aspect (unless approved to exclude, or impact is nominal on organization). For major changes, this will generally include communication, training, process change. • System development for large financial system projects is monitored via Steering Committees, Quality Assessments, and via CIO development controls, to ensure key activities are executed. • For key financial systems, consideration of control impacts are explicitly considered.
Rapid Growth is monitored & budgets revised accordingly	Growth & Strategy; Global Business Operations; HR	• Internal budgets & non-financial targets are set in consideration of ABC Company's strategy; monitoring considers low resources as well as excess resources.
	Finance Operations	• As noted earlier, Budgets are revised quarterly & growth can be accommodated based on business need.
	CIO	• CIO spend is guided via an IT Steering Committee that considers growth, and ABC Company's strategy in assigning budgets & resources.

COSO Change Management Area	Responsible	ABC Company Activity
New Technology is monitored to assess impact on organization	CIO	• CIO strategy (updated periodically) considers external developments; the strategy considers new developments in technology.
New Products or Acquisitions are monitored for impact	Operating Groups, Growth Platforms	• New service lines (service offerings) are monitored for financial & market success. • New skill needs are monitored & communicated to Recruiting (for external acquisition) & Training (via internal capability building plans). • Impacts of new services lines & new skills are monitored via standard reporting (for example, expansion into outsourcing included assessment of impacts on consulting service fees).
	Finance Operations	• Overhead allocations (& other related financial reporting mechanisms) are adjusted annually to consider new product lines, other changes.
	P&L Entities, HR, Global Controllership, etc.	• Acquisitions are reviewed and monitored by a variety of teams — Financial performance is monitored by the P&L entity to which the acquisition reports; HR reviews the compensation & benefit plan of the acquisition, Global Controllership monitors financial reporting, etc. Acquisitions go thru a through a due diligence process, which includes legal, compliance, ethics, and business reviews.
Corporate Restructuring activities are managed to minimize disruption	Global Business Operations Legal, HR	• Macro level staff reduction areas are reviewed by HR leadership to ensure planned service reductions do not adversely impact operations and are in compliance with local laws.
	Business Leads	• Business Leads and local control leads remain responsible for assigning controls responsibilities to new personnel in the event of restructuring.
	Unit leadership	• Morale is monitored via the Global Employee Surveys, with monitoring or improvement goals set by each entities leadership.
	CIO, Facilities & Services	• Once employees are removed, access (physical, logical) is quickly revoked.
Global Operations are monitored to ensure changes are identified	Managing Directors	• Managing Directors are responsible for monitoring the local environment & raising issues.
	Legal	• Local Legal personnel monitor local regulatory environments, raising issues to Legal leadership as needed.

COSO Change Management Area	Responsible	ABC Company Activity
	Global Asset Protection	• At the corporate level, an ABC Company security team monitors trouble areas; maintaining evacuation plans and backup communication plans as needed.
	Various	• Results in local operations are monitored by the appropriate P&L entity or cost center entity.

Monitoring

15. Monitoring is a continuous process that management uses to assess the quality of internal control performance over time. At the highest level, Monitoring encompasses normal monitoring activities, periodic evaluations or monitoring, and the reporting of deficiencies to the appropriate level of management and the board of directors.

16. At the summary level, the COSO framework outlines several areas of focus that should be considered in order to ensure effective monitoring:

Area of Focus	ABC Company's Expectations
Ongoing Monitoring	• Extent to which personnel, in performing their normal activities, obtain evidence that the system of internal controls is functioning — for example – Operating Management compares sales, production, etc. data obtained daily to system generated data – Data used to manage operations is reconciled with data generated by financial system – Operating Personnel sign off on the accuracy of their units' financial statements & are held responsible if errors are discovered • Extent to which communications from external parties corroborate internally generated information – Customers corroborate billing data by paying on time – Communications from vendors are used as a monitoring technique – Controls that should have prevented or detected problems are assessed • Periodic comparison of amounts recording by the accounting system with Physical Assets – Inventory levels are checked when goods are taken for shipment; differences are corrected – Securities held in trust are counted periodically & compared to records • Extent to which training seminars, planning sessions and other meetings provide feedback to management – Relevant issues raised at seminars are captured – Employee suggestions are communicated upstream

Area of Focus	ABC Company's Expectations
Ongoing Monitoring (continued)	• Whether personnel are asked periodically to state whether they understand and comply with the code of conduct, or whether signatures are required to evidence performance of critical control functions • Responsiveness to internal & external auditor recommendations – Executives with appropriate authority decide which recommendations will be implemented – Desired actions are followed up to verify implementation • Effectiveness of internal audit activities; appropriate IA staffing, competence & experience; position within organization is appropriate; access to BOD or Audit Committee is appropriate; their scope is appropriate to the organization's needs
Periodic Monitoring/ Separate Evaluations	• Scope and frequency of separate evaluations of the internal control system, including whether appropriate portions are evaluated; evaluations are conducted by individuals with appropriate skills; scope, depth and frequency are adequate • Appropriateness of the evaluation process, including whether the evaluator gains sufficient understanding of the activities; analysis is made vs. established criteria • Appropriateness of the methodology for evaluating whether the system is logical and appropriate, including standard methodology (such as checklists, tools); coordinated planning effort for the evaluation process; evaluation process is managed by an executive with appropriate authority • Appropriateness of level of documentation; are policy manuals, org charts, operating instructions, etc available; is the evaluation process documented?
Reporting Deficiencies	• Existence of a process for capturing & reporting identified deficiencies — from external sources & from ongoing monitoring or separate evaluations • Appropriateness of reporting protocols — are deficiencies reported to the person directly responsible for the activity, and to a person at least 1 level higher? • Specific types of deficiencies are reported to senior management and to the board • Appropriateness of follow-up activities. Is the underlying event corrected; are causes of problems investigated; is follow-up action taken to ensure corrective action?

Monitoring Activities

17. Monitoring stands as both an integrated set of activities ***and*** a standalone set of assessment activities. This provides both ongoing assurance of controls and a separate and distinct set of feedback to management on control operations.

Ongoing Monitoring — Financial

- Operating Group Chief Executives sign off on the accuracy of their financial results.
- Senior Executives are measured on GAAP compliance and internal controls compliance; this is a formal metric included in Senior Executive measures & influencing compensation & rewards. GAAP failures and internal controls failures negatively influence the Senior Executive evaluation. GAAP compliance information is provided by Corporate Controllership; Control execution information is provided by Internal Audit & the 404 Core team.
- Control activities include a balance of transactional & monitoring controls throughout the organization.
- Regular (quarterly) feedback on operation of critical controls is provided (independent of testing of those controls).
- Internal Controls require appropriate evidence, including a number of approvals (usually electronic) on key activities. Management's training & communication on this point is clear; evidence is required to be retained to prove execution & increase certainty of financial reporting.
- Corporate Controllership monitors key GAAP pronouncements, and adjusts and communicates finance policies as required.

Ongoing Monitoring — Internal & External Audit

- External audit recommendations are assessed by the Chief Accounting Officer (CAO) and others as needed; implementation is tracked by Global Controllership.
- Internal Audit reports to the Audit Committee, and administratively to the Chief Risk Officer, outside of the Finance organization.
- The Internal Audit plan is approved by both senior management and the Audit Committee, with corresponding staffing to execute the plan.
- Internal audit recommendations are reported to the CFO, CAO and others as appropriate; the management of each entity is required to respond with an action plan to IA points. The unit responsible for implementing the recommendations executes quarterly tracking through implementation.

Ongoing Monitoring - Operational

- Forums exist to compare operating information to financial information — for example, the Executive Leadership Team meetings, and the Operations Council.
- Performance monitoring (via the forecast, analysis of variances) occurs at each P&L or cost center node on a quarterly (minimum) basis.
- Collection (Days Sales Outstanding) is relatively low, indicative of rapid customer payment and a low billing error rate (among other factors).

Ongoing Monitoring — Compliance and Regulatory Matters

- The Compliance and Regulatory Matters (C&RM) team monitors multiple aspects of operations within the company through methods such as: monitoring the Business Ethics Help Line, conducting multiple ethics and compliance surveys conducted on a periodic basis for longitudinal comparability.
- Integrate with other teams, such as the Internal Audit team, to leverage their assets for additional specific monitoring requirements.

Separate Control Activity Evaluations

- Evaluation activities are planned for all quarters, though the scope of each quarter may differ. The design of our controls is evaluated every year, and every control activity goes through an assessment at least once in a year.
- Evaluation activities are planned and monitored by the core team.
- Control evaluation activities are executed by individuals who are not responsible for operating a control; they receive independent training on how to conduct their assessments.
- Assessments are conducted using a standardized set of test plans, which may be modified to reflect local conditions.
- Test plans are created to provide a substantive body of evidence that supports execution; sample size guidance ensures appropriate testing levels to provide management comfort of execution (with adjustment permissible by management).
- Assessment results are reporting to the Business Lead and to the Internal Controls team via a portal, with test results documented in the portal.
- Confirmation activities (or "roll forward" activities) are planned for the 4th quarter.

- Internal Audit also evaluates controls as part of its standard audit activities for an entity.

Reporting Deficiencies

- Ongoing control failures identified locally are assessed for Significant Deficiency or Material Weakness potential using a set of guidelines reviewed by the Internal Controls Steering Committee and the Audit Committee (at the summary level).
- Control failures (with no compensating controls) that have potential to create a significant deficiency or material weakness are elevated to the Chief Accounting Officer, CFO, General Counsel and the Disclosure committee, and summarized for the Audit Committee.
- Control failures are tracked until confirmation is received that they have been resolved. The core team monitors failure resolution to ensure reasonableness.

Quarterly and Annual Management Representations

Related to Example 38:

Notes about the material

Management of this international manufacturing company uses the following line-management certification form to:

- Communicate a tone from the top regarding management's expectations about the quality of financial reporting
- Establish ownership of meaningful financial reporting risks and related key controls throughout the organization
- Routinely receive acknowledgement, through self-assessment by line managers, regarding the effective operation of key controls

Table of Contents

Background and Instructions

1. The CEO and CFO are required to make an evaluation of disclosure controls and procedures in connection with the filing of Forms 10-Q and 10-K with the U.S. Securities and Exchange Commission. Responses contained in the attached questionnaire will be used in their evaluation of disclosure controls and procedures in connection with the following report:

Form 10-Q for the quarterly period ended March 31, 20XX

2. Please Note: your responses to this questionnaire are intended to support and provide reasonable assurance that certifications made by the CEO and CFO to the Securities and Exchange Commission, the Audit Committee and our shareholders are correct and accurate. Certain of these certifications, if incorrect, could result in severe penalties including criminal penalties. You should respond to this questionnaire as if you were making these certifications yourself and as if penalties could apply to you personally (in some cases they can).

3. This questionnaire is an integral part of the evaluation process. You are primarily responsible for answering the following questions for the line of business and/or functional area(s) of the Company that you supervise. Answers should be based upon the knowledge that a reasonable person might conclude you should have as the manager of the area(s) that you supervise. Please note: if you are aware of a reportable item that does not fall within your functional area of responsibility, you should still report it. Do not assume that someone else has reported it on his or her questionnaire.

4. Please review each question and respond by marking either Yes, No or N/A. Unless otherwise indicated, all questions require a response. Explanations should be provided for all "No" all "N/A" responses for which the reason is not obvious, except for questions B.8, G.16 and H.7, which require explanation if "Yes" or "N/A" answers are provided. The explanations are to be provided in the area beginning on page 9. Attach any information or documentation that you feel is appropriate and relevant to support your response(s).

5. Many of the questions address materiality. For purposes of this questionnaire, unless otherwise indicated, use your judgment for what is considered material. A series of related transactions should be combined when determining materiality. Any transaction or event that might cause a violation of a loan covenant or which involves fraud should always be considered material regardless of the dollar amount. Any question that involves the override, suspension or effective operation of a control procedure should be considered material if it could be considered reasonably likely to result in a material affect now or in the future.

6. You should report any situation that has occurred since the end of the most recent year-end or quarter that was not reported on a previous questionnaire.

7. Your responses to the questions contained in the attached questionnaire should relate directly to the plant site for which you are responsible.

8. This quarterly and annual management representation, including the acknowledgment and signatures that follow, should be emailed to _____ by the following deadline:

April XX, 20XX

9. If you have questions regarding how to respond properly to particular questions contained in the questionnaire, you should direct them to the Corporate Controller.

Acknowledgment and Signatures:

10. We recognize that we hold important roles in the disclosure controls and procedures of the company, and that information we provide is used in the company's quarterly and annual filings with the U.S. Securities and Exchange Commission. We confirm that the responses to the questions contained in this memorandum, as well as any additional notes or attachments, properly reflect our representations:

Name: ________________________________

Title: ________________________________

Date: ________________________________

Name: ________________________________

Title: ________________________________

Date: ________________________________

Quarterly and Annual Management Representations

	Yes	No	N/A
A. Significant Accounting Policies — Revenue Recognition			
1. For all sales recognized during the period:			
a. Was there persuasive evidence that a sales arrangement existed between our customer and us prior to the end of the period?			
b. Had the products been delivered or had the services been rendered prior to the end of the period?			
c. Was our sales price fixed or determinable prior to the end of the period?			
d. Was collectibility from our customer reasonably assured prior to the end of the period?			
2. Were all significant sales transactions of a normal, recurring nature?			
3. Were the product mix, nature of customers, terms of sale, credit policies, and related items similar to those of prior periods?			
B. Significant Accounting Policies — Other Than Revenue Recognition			
1. Have interplant transactions been accounted for in designated general ledger accounts?			
2. Have the results of joint ventures in which the company does not have a controlling financial interest been included in the general ledger using the equity method of accounting?			
3. Have the general ledger accounts been translated (or remeasured) from local currency to the U.S. dollar at rates of exchange issued by Corporate Finance on a monthly basis?			
4. Have all expenditures related to new product development been charged to expense as incurred?			
5. Has the cost basis of inventories been determined on a first-in, first-out basis?			
6. Has property, plant, and equipment been capitalized and depreciated in accordance with companywide guidelines established by Corporate Finance?			
7. Were items not meeting the criteria for capitalization expensed?			

	Yes	No	N/A
8. Have there been any events or changes in circumstances that indicate the carrying amount of a long-lived asset may not be recoverable? Triggering events that you should consider include: – Significant decrease in the market price – A significant adverse change in legal factors or business climate – Accumulation of significant excess costs beyond original expectations for assets constructed or acquired – Continuing operating cash flow loss associated with the asset use – Expectation of sale/disposal significantly before the end of the established useful life			
C. Judgments and Estimates — Allowances for Doubtful Accounts			
1. Have accounts receivable balances that are more than 60 days past due been reviewed at or near the end of the period for purposes of forming judgments as to the likelihood of collectibility?			
2. Has trend information been reviewed within the last 12 months to determine whether a normal and predictable pattern of accounts receivable write-offs exists?			
3. Has an allowance for doubtful accounts been established in an amount equal to the sum of:			
a. The amount of specifically identified accounts receivable balances whose collectibility is doubtful; and			
b. The best estimate of the remaining accounts receivable balances whose collectibility is doubtful?			
4. Have you considered whether any factors have occurred since trend information was last reviewed that would influence the “best estimate” referred to in question C.3.b?			
5. Have provisions and write-offs that are related to credit issues been charged to bad debt expense?			
6. Have provisions and write-offs that are related to pricing (such as for rebates or volume discounts) or other matters of disputes settled in the customer’s favor been charged as a reduction to sales?			
D. Judgments and Estimates — Reserves for Inventories			
1. Have reserves been established to reduce the carrying value of inventories to its net realizable value whenever the quantity on hand exceeds expected demand?			
2. In establishing the reserves referred to in question D.1, have inventory usage reports (such as “two years no usage”) been reviewed in the most recent fiscal quarter (or more frequently)?			

	Yes	No	N/A
3. Have reserves been established to reduce similar types of inventory to its net realizable value, regardless of demand, whenever the aggregate carrying value is more than the aggregate market value of that inventory?			
4. Have you considered whether there have been any decreases in the market value of inventory that would trigger an evaluation of the need for the reserve referred to in question D.3?			
E. Judgments and Estimates — Warranty Accruals			
1. Have warranty accruals been established for specifically identified warranty issues that are probable to result in future cost?			
2. Do the specific warranty accruals referred to in question E.1 reflect the best estimate of the future costs?			
3. Have the specific warranty accruals referred to in question E.1 been reviewed at or near the end of the period?			
4. Has a warranty accrual been established on a non-specific basis for estimated remaining future costs that will be incurred on product that was sold through the end of the period?			
5. In establishing the non-specific warranty accrual referred to in question E.4, was trend information reviewed in the most recent fiscal quarter (or more frequently)?			
6. In establishing the non-specific warranty accrual referred to in question E.4, have extended warranty obligations been given special consideration?			
7. Has care been taken not to over-provide for warranty costs by inadvertently doubling up on accruals in both the specific and non-specific portions of the warranty accrual?			
F. Judgments and Estimates — Accruals for Loss Contingencies			
1. Have all loss contingencies been accrued for when a future loss is probable and the amount can be reasonably estimated? (A “loss contingency” is an existing condition, situation, or set of circumstances involving uncertainty as to a possible loss to the company that will ultimately be resolved when one or more future events occur or fail to occur.)			
2. Have all accruals for loss contingencies been reviewed at or near the end of the period?			
3. Have all known loss contingencies been communicated to Mark Hartman, the Corporate Controller?			

	Yes	No	N/A
G. Internal Accounting Control Systems			
1. Have basic internal accounting controls been established and maintained, giving careful thought to segregation of duties, to ensure the validity, accuracy, and completeness of recorded transactions?			
2. Have appropriate cut-off procedures been established and maintained to ensure proper recognition of revenues and expenses in appropriate fiscal quarters, and to properly reflect assets, liabilities, and equity at the end of each fiscal quarter?			
3. Has detailed information been reconciled to the general ledger control accounts on a monthly basis for:			
a. Cash?			
b. Accounts receivable?			
c. Inventories?			
d. Accounts payable?			
e. All other accounts with significant activity?			
4. For accounts that do not have significant activity:			
a. Was there a clear understanding of the details of the account balances at the end of each fiscal quarter?			
b. Was the detailed information for such accounts reconciled to the general ledger control accounts on a periodic basis (at least annually)?			
5. Have interplant accounts been reconciled on a monthly basis?			
6. Have reconciliations of cash balances on bank statements to our internal accounting records been performed on a timely basis after receiving those statements?			
7. For all reconciliations, were all reconciling items investigated in a timely manner and of the type and amount that would be considered normal and recurring?			
8. Have internal financial records been reviewed analytically by financial management as a means to highlight potential failures of basic accounting controls that may need to be investigated and resolved?			
9. Are managers of the company provided with financial reports that:			
a. Enable them to monitor performance?			
b. Provide them the ability to form judgments about the validity, accuracy, and completeness of reported amounts?			
10. Have controls been established and maintained to ensure that assets and the accounting records are adequately safeguarded to prevent loss or theft?			

	Yes	No	N/A
11. Have approval and responsibility levels been established for all business transactions to ensure that transactions are executed in accordance with management's authorizations?			
12. Are the approval levels referred to in question G.11 at least as restrictive as necessary to meet corporate requirements?			
13. Has corrective action been taken to address all known instances of noncompliance with internal accounting control procedures, whether intentional or unintentional?			
14. Have all recommendations for changes in internal accounting control procedures resulting from corporate internal audit or Management's Assessment of Internal Control Over Financial Reporting activities been implemented in accordance with established timelines?			
15. Have all recommendations for changes in internal accounting control procedures that resulted from **external audit activities** been implemented or, if not, has an implementation plan been discussed **and agreed to** with the Company's Director, Internal Audit?			
16. Have there been any significant changes to the system of internal accounting controls?			
17. If the answer to question G.16 is "Yes," have the significant changes to the system of internal accounting controls been discussed with and agreed to by the Company's Corporate Controller?			
H. Other Representations			
1. Have all leases been reviewed to ensure they are operating leases rather than capital leases?			
2. Are all procedures associated with accounts payable and accrued expenses consistent with the procedures used for previous quarters?			
3. Are the methods used to allocate expenses between and among quarterly periods (on the basis of revenue, benefits, time or activity association) consistent with the methods used for previous quarters?			
4. Are expense classifications consistent with prior year-end classifications?			
5. Has complete and accurate information been provided to Corporate Finance when requested?			
6. Have all financial records and related data been made available to our independent registered public accounting firm?			
7. Based on your knowledge, are you aware of any of the following:			
a. Weakness in internal control that could lead to material losses or reporting errors?			
b. Fraud or defalcation, regardless of materiality, involving a Company manager or an employee with a significant role in internal controls?			

	Yes	No	N/A
c. Material transactions which you have reason to believe may not be accounted for in accordance with accounting principles generally accepted in the United States?			
d. Unresolved Ethics Policy violation?			
e. Violations of security or other laws or regulations that could have materially adverse consequences?			
f. Material instances where business system generated results have been overridden?			
g. Material completed transactions that have not yet been recorded on the Company's books?			
h. Incomplete or pending transactions that have prematurely been recorded on the Company's books?			
i. Changes in material assumptions that are used in the application of any accounting method that have not previously been discussed and cleared through Corporate Finance?			
j. New off-balance sheet relationships, long-term contracts, lease commitments, employment contracts or similar arrangements that obligates or contingently obligates the Company in a material amount?			
k. Material transactions that are unusual, non-recurring or otherwise outside the Company's normal course of business?			
l. Material title defects to any Company-owned assets?			
m. Material violations or breaches in any contractual obligations of the Company?			
n. Issues raised by regulators or tax examiners that could result in materially adverse consequences?			
o. Instances where the Company's assets have been pledged as collateral?			
p. Other item(s) that is not otherwise covered in this questionnaire that could materially affect the Company's results of operations, or cash flows for the period, or the carrying value of its assets or liabilities or its financial condition at the end of the period?			

Explanations

11. Provide below explanations for all “No” and “N/A” responses, with the exception of questions B.8, G.16 and H.7, which require explanation if “Yes” or “N/A” response is provided.

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Question #

Quarterly and Annual Disclosure Committee Review Procedures Checklist

Related to Example 38:

Notes about the material

This international manufacturer has formed what it refers to as a Quarterly and Annual Disclosure Committee (QADC). This committee uses the following checklist to ensure that they have reviewed and considered information about risks and controls in areas of identified meaningful risk.

At the end of each quarter the QADC will:

Review and discuss the following:

- CEO/CFO evaluation of disclosure controls and procedures and comments relevant to evaluation document;
- Summary of responses to annual and quarterly management representations (see Appendix B);
- Summary of quarterly changes to design of internal control over financial reporting;
- Areas of significant process variation (at least once a year — if this review was not completed in the current quarter, indicate when it was last completed);
- Review of the scope of management's evaluation (financial analytics and qualitative review to determine the scope of management's review of internal control over financial reporting; and
- Review of management assessment status reports (plan for the testing of the operating effectiveness of internal controls over financial reporting, as well as other audits of the organization) and summary of control deficiencies (SOCD) (results of tests of the operating effectiveness of internal controls over financial reporting.)

Review a written or oral summary of the following:

- Pending or threatened litigation, claims, and assessments;
- Summary of relevant ethics hotline communications and the business conduct and oversight committee violation reporting tracking;
- Internal audit/risk assessment status, including completed projects and status of findings/disclosures;
- Restructuring/reorganization activities;
- Communications/issues with outside auditors;
- Global policy review process status; and
- Any other matters relevant to forming the conclusions noted below.

As a committee, form conclusions regarding the following:

- The effectiveness of disclosure controls and procedures as of the end of the period covered by each Form 10-Q and Form 10-K (include the conclusion in the report to the CEO and CFO);
- The effectiveness of internal control over financial reporting at the end of the fiscal year, separately considering design effectiveness and operating effectiveness (this procedure is applicable only in the final quarter of the year — include the conclusion in the report to the CEO and CFO); and
- Whether any material changes were present in internal control over financial reporting or other disclosure controls and procedures during the quarter most recently ended (include any such changes in the report to the CEO and CFO).

Prepare the following written documentation:

- Agenda and conclusions for committee's report to CEO and CFO; and
- Documentation review notes to be distributed to preparers of documentation reviewed as part of the meeting.

Enterprise-Wide Risk Matrix

Related to Example 18:

Notes about the material

The following risk matrix contains excerpts from multiple places within a retail chain company's larger enterprise-wide risk analysis. It is presented only to demonstrate a possible format for a formal risk analysis that might also be used to assign monitoring responsibilities. It also demonstrates how the organization identifies and considers changes to risks between periods.

Note that these excerpts are not intended to, and do not present all of the risk considerations this company considered in each area.

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
1	Sales											
	Same-Facility Sales Growth	Strategic	CEO		Grow core business to achieve 1-2% same-facility growth	Reduced customer spend at facility maturity; 3-5 years in life cycle	H	5	H	5	Introduction of new products and services; Tighter collections which reduce retrievals and time needed for credit activities; Effective advertising	
						Unfavorable legislation	H	5	L	1	Lobbying efforts; Legal department oversight	
						Operational inconsistency - execution, lack of accountability, facility appearance, entrepreneurial culture, training, pool of job applicants	H	5	M/H	4	Improved training programs; Utilization of the learning management system	
						High turnover and lack of skilled and tenured managers	H	5	M/H	4	HR initiatives implemented in 2006/2007 to address turnover	
						Increased product deflation and lack of new or attractive product offerings	M	3	H	5	Reducing term and price to move product	
						Increased competition	M	3	M	3		
						Poor inventory management at the facilities	H	5	M	3	Inventory management controls: Facilities required to perform inventory two times/week; District Managers to perform inventory once per quarter; System controls in place that limit purchasing; District Manager manages the mix to ensure the right items are in the facility	
						Shrinking customer discretionary income due to higher prices for gas, utilities, other	M	3	H	5		
						Ineffective integration with Financial Services	M	3	M	3		New risk
	Competitive Intrusion Plan	Strategic	VP Operations and VP Strategic Development		Implementation and execution of a competitive intrusion plan to protect market share	Lack of willingness by the company to invest the resources in a plan	M	3	M	3	Hired a director to develop the program; Current pilot test	New objective

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
2	Consistency of Operations of Facilities											
	Consistency of Operations of Facilities	Operational/ Strategic	COO		Ability to execute at the facility level, close the sale, and maintain customer base	Not hiring people with the right attitude, characteristics and skill set	H	5	M/H	4	Two staff screening coordinators per division; In-house sourcing of candidates; On-line applications; Employee pay plan which provides raises every six months; On-line employee training and tracking	
						Not having the right product (mix of new and refurbished, colors, size)	H	5	M	3	Ability for each facility to look up inventory at all area facilities; Auto-order and ship product directly to the facility to support upcoming advertisement; System min/max inventory levels	
						Collection percentage out of line with company goals	H	5	L	1	Daily monitoring of collections standards/goals to actual; Automated account management system; Increased focus	Rating for probability was M
						Lack of good customer service	H	5	M/L	2	1-800 customer service number with monitoring against standards; Customer service-oriented facility employees; Providing quality products to the customer; Sales training course rolled out in 2007; Customer satisfaction surveys utilized	
3	Customer Focus and Customer Service											
	Customer Experience	Strategic	Strategic Planning		Defining what the complete customer experience should be	Lack of understanding of how to operationalize our segmentation knowledge of the customer; not enabling a 2nd transactional channel	M	3	M	3	Marketing study on customer experience	
	Quality Customer Service	Operational	Operational Services		Timely and effectively address customer concerns and inquiries within 24 hours for an initial response and 4 business days to resolve and close the case	Lack of qualified personnel and an inadequate customer service system	M	3	M	3	Former Ops specialist heading the department	Rating for probability was L - concern about enough qualified staffing to handle the work
						Lack of confirmation with customer that issues were resolved	M	3	M	3		
						Lack of proactive customer-satisfaction contact by facility personnel	M	3	M	3		

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
4	**Product Services**											
	Product Service and Repair	Operational	Manager Operational Services; Manager Product Services		Timely repair and return of product to the facility within 7 days of receipt in a cost-effective manner	Not having parts needed to perform the repair (i.e., parts unavailable from manufacturer or not ordering parts timely)	H	5	L	1	Return authorization process (Vendor repurchase of non-operating items); Selection of vendors with high-quality products and excellent technical support of those products; Analysis of stock replenishment reports for each product service center; Inventory system min/max; Seven-day follow-up process for all parts ordered; Authority to expedite or make purchases from local merchants for back-ordered parts; Home office follow-up on back-order or slow-ship parts	
			Manager Operational Services; Manager Product Services			Aging management team to supervise service staff	M	3	M	3	Ongoing succession planning; Recruitment of younger employees; Added Assistant Manager position in 2007	
						Limited personnel with appropriate technical expertise	M	3	M	3	In-house on-the-job training program	
			Manager Product Services			Not capturing all potential revenue (vendor warranty, return authorization, receivables for non Company repairs) to offset cost	L	1	L	1	Checks and balances at the product service center to identify product warranty opportunities; Billing and monitoring process for non-Company repairs; Home office monitoring of warranty claims and return authorization credits to ensure payment	
			Manager Product Services			Unanticipated increase in costs (i.e., product parts, fuel, utilities)	M	3	M	3	Purchasing of manufacturer certified refurbished parts; Salvaging parts from out-of-service products; Education of operators (i.e., fuel costs, operating safety); Tracking management device for service vehicles to be tested in 2008 (tracks idle time, mileage, etc.)	
5	**Fleet Management**											
	Effective Fleet Management	Operational	Manager Operational Services		Cost-effective utilization of fleet	Ineffective maintenance program	M	3	L	1	Vehicle maintenance program with cost savings of $1.3m; Preventative maintenance program in-progress	
						Failure to maintain licensing and inspection requirements	L	1	L	1	Outsourced licensing and inspections to third-party vendor	
						Inability to provide options to match type/ size of vehicle to product delivered	L	1	L	1	Multiple sizes of vehicles now available	Rating was M & M - now have multiple sizes of vehicles available
						Keeping vehicles past useful life	L	1	L	1	Centralized auto-aging program	

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
			Manager Operational Services			Rising costs of fuel, replacement parts and maintenance costs outside of warranty repairs	M	3	M	3	Increase in warranty with vehicle manufacturer (5yr/50,000 miles); Signing 60-month leases and liquidating at 36 months	New risk
	Appearance of Fleet	Reputational	Manager Operational Services		Maintain high-quality appearance of vehicles	Poor appearance of vehicle due to damage, failure to keep clean, failure to keep updated branding, etc.	M	3	M	3	Quarterly district manager inspection and facility-appearance check lists	
6	**Real Estate**											
	Lease Negotiations	Operational	Manager Operational Services		Provide support to field operations through effective and timely lease negotiations	Not having sufficient resources to adequately negotiate key leasing elements (i.e., signage, lease price/terms, approval of programs)	M	3	L	1	Fully staffed and cross-training in place	Rating for Impact was M - Real Estate dept has appropriate resources, cross-training of employees, etc.
	Acquire Facility Sites	Operational	Manager Operational Services		Acquire and maintain facility sites to support facility operations and effective management of capital funds	Poor oversight of construction costs by Operations (bad business practices) and District manager acting as general contractor for the build-out without sufficient skills	M	3	M	3	Two home-office construction managers support field questions; Construction Manager test in 2008, one hired for 2008 for the field; One construction manager dedicated to subsidiary; New contractors are screened by the home office; field cannot use a general contractor unless approved by home office	Combined last year's objective 16 & 17
						Insufficient data to determine real estate needs	L	1	L	1	Lease administration system	Rating for impact and probability was M - Real Estate dept has necessary data from the lease administration system
						Non-compliance with purchase order approval policy	L	1	L	1	Vendor management system	
	Lease Administration System Management	Operational	Manager Development		Effective management of lease administration system	Untimely or inaccurate receipt and input of lease information into the lease administration system	L	1	L	1	Abstract and data-entry review process; Restricted access to the lease administration system	
						Lack of resources with appropriate skill set needed to maintain the lease administration system	L	1	L	1	Cross-training of employees	Rating for impact and Probability was M - Real Estate dept has appropriate resources, cross-training of employees, etc.
7	**Financial Reporting**											
	Financial Reporting	Financial /Compliance	CFO		Timely, accurate and compliant financial statement reporting (GAAP)	Staying abreast of accounting implications related to new business and changes	H	5	L	1	Subscriptions are maintained to obtain access to technical pronouncements; Disclosure committee review; Audit Committee review; Review by inside and outside counsel	

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
						Maintaining qualified staff	H	5	L	1	Employee training; SOX testing, remediation and reporting to Audit Committee; Effective Audit Committee oversight over financial reporting	Rating for probability reduced from M - additional resources
						Inaccuracy of data from IT systems that impact financial reporting (i.e., staffing, inventory tracking, and financial)	H	5	L	1	Automated interface; Account reconciliations	
						Inaccurate accruals (tax reserve, worker's compensation, litigation, payables, vacation accruals)	H	5	M/L	2	SOX quarterly testing to monitor controls in place; In-house expertise, outside vendor analysis	Rating for probability reduced from M - additional resources
	SEC Filing & Non-GAAP reporting	Financial /Compliance	VP Legal & Compliance		Conduct timely and accurate SEC filing and reporting (i.e., 8-K, press releases, non-GAAP disclosures)	Lack of knowledge of required SEC reporting disclosures	M	3	L	1	Disclosure committee review; Audit Committee review; Certification process; Review by outside counsel	Rating for probability reduced from M - additional resources
8	FAS 109 Compliance											
	FAS 109-FIN 48	Financial/ Compliance	CFO and VP Taxation & Compliance		Compliance with FAS 109 and FIN 48	Lack of knowledge/understanding of accounting pronouncements, tax laws, and their impact on the sustainability of tax positions	H	5	M	3	More experienced, knowledgeable, tenured tax personnel; Subscription to tax research services; Use of outside tax consultants as appropriate	
						Lack of support and documentation of tax positions	H	5	M/H	4	Increased focus on documentation throughout the tax department	
9	General Accounting											
	Inventory Management	Operational	Manager Inventory Management		Ensure timely and accurate payment of vendor invoices for inventory purchased for resale in the facilities	Facility not acknowledging receipt of merchandise in inventory tracking system in a timely manner (i.e., within 24 hours of delivery)	M	3	M	3	Follow up with the facilities for items not yet received in inventory tracking system; Proof of delivery obtained from vendor by the home office	Rating was H & H - audit results and the quantity involved versus the total population
						Improper 3-way match (wrong PO to invoice), invoice price and PO price not matching or duplicate payments	L	1	L	1	System restrictions in inventory tracking system; Follow-up by merchandising with vendor on PO and invoice price differences; System warnings in inventory tracking system	

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
						Facility incorrectly recording receipt of merchandise in inventory tracking system (i.e., wrong PO, incorrect quantity)	L	1	L	1	Three-way match performed by inventory accounting	
						Lost invoices	L	1	L	1	Unbilled-invoice review; Monthly, weekly vendor invoice reporting (most invoices are sent electronically via PDF or word document); Vendor statement review	
						Inventory is costed at the improper amount or incorrectly expensed	L	1	L	1	Facility will notify someone in Inventory Department at time of charge-off if the remaining value was too high; Review of unattached invoices; Inventory Supervisors must approve any expense hitting the facility that is greater than $500	New risk
10	**IT Systems**											
	Company IT Technology and Systems	Operational	CIO		Providing effective technology and systems with functionality that supports the company's needs (i.e., financial, operational, compliance)	Lack of modernized integrated systems	H	5	M	3		
			CIO			System-development infrastructure is not adequate/ non-responsive to the business	M	3	H	5	Systems development life cycle process in place, although more adequate for smaller-scale projects	Updated mitigating control for systems development life cycle process in continued support of H probability for 2008
			CIO			Inability to determine long-term growth limitations related to staffing	M	3	M	3	Hired VP of Accounting with responsibility to evaluate financial needs and capabilities of staffing system to meet these needs	
			CIO			Current limitations (i.e., functionality and access to data) with existing inventory tracking, financial, staffing systems and RSSS	M	3	M	3	Ongoing implementation of the data warehouse and business information function	Added RSSS to risk

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
			CIO			Ineffective communication between the business and IT	H	5	M	3	Strategic planning committee which meets periodically; IT steering committee	
			CIO			Lack of effective quality control process for upgrades and implementations (i.e., ineffective tools, inadequate infrastructure and limited resources)	H	5	H	5	Change control, release management, as well as configuration management processes are in progress; QA analysts to assure testing has taken place	
			CIO			Vendors do not accurately and timely develop needed application changes to support business and compliance needs (i.e., inventory tracking, financial, staffing, RSSS)	H	5	M	3		Added RSSS to risk
11	**IT Security**											
	IT Compliance	Compliance/ Operational	CIO		Ensure IT operations comply with all federal, state and industry laws and regulations	Non-compliance with personal-confidential information standards associated with payment integration with inventory tracking system	H	5	M	3	Currently at Level 2 compliance, with Level 1 compliance required in 2008	Rating for Probability was H - added the mitigating control as support
						Lack of integration and collaboration of home office functions that impact security and risk management (IT security, building security, H/R, loss prevention, risk management, internal audit, legal)	M	3	M	3		
						Current limitations with existing inventory tracking, financial, staffing systems, and RSSS	M	3	M	3		Added RSSS to risk
						Lack of modernization and integration of existing infrastructure	H	5	L	1	Investment in IT infrastructure (i.e., networks and MPLS)	Rating for Probability was decreased to L - added mitigating controls as support
	IT Security	Operational	CIO		Provide a secure infrastructure in which malicious attacks have no impact on the business	Unknown infrastructure vulnerabilities	H	5	M	3	Periodic vulnerability assessments; Patch management	
						Constantly changing external security threats	H	5	H	5	Utilization of a layered defense strategy: anti-virus software, firewall and intrusion detection system	

Field Operations 2008 Risk Matrices

	Heat Map Category	Objective Type	Domain/ Interviewee	Objective/ Category	Objective	Risks	Impact		Probability		Mitigating Controls Discussed	Notes Regarding Significant Changes from 2007
12	IT Infrastructure and Support											
	IT - Infrastructure	Operational	CIO		Providing IT technical infrastructure (i.e., servers, email) for company to decrease downtime and improve connectivity	Lack of long-term IT infrastructure road map/ plan	H	5	M	3	Development of a long-term infrastructure plan in progress; Implemented considerable infrastructure changes with move to the new building	Updated verbiage for IFS changes
						Lack of modernization and integration of existing infrastructure	M	3	L	1	Incorporation of important environmental features into the infrastructure, while substantially modernizing our core networking functionality with move to the new building	Rating for probability was decreased to L - added mitigating controls as support
						Inability to manage outages/problems associated with outdated infrastructure	M	3	M	3	Existing operating procedures related to system monitoring and failures	
						Inability to grow the infrastructure parallel with the growth of the company	M	3	M	3	Increased capacity to adequately address company growth with implementation of new infrastructure	Rating was H & H - added mitigating controls as support
					Ensure cost-effective, continuous system availability	Lack of effective quality control process for changes / patches	H	5	M	3	Weekly change management process review; Implemented policy that requires all patches moved into production to be logged as security events	Rating for probability was H - added mitigating controls as support
						Inability to proactively monitor system capacity and performance	M	3	H	5		
						Inadequate resources to support critical applications	H	5	M	3	Increased resource capacity by adding additional personnel; Increased skill set and knowledge base of existing employees	Rating for probability was H - added mitigating controls as support
	IT Support	Operational	CIO	Operational	Effective IT support group	High turnover and or not having adequate bench strength for IT support	M/H	4	M	3	Increase bench strength over the past year via the hiring of new personnel and increase in experience and knowledge of existing personnel	Rating was H & H - added mitigating controls as support
						Lack of communication within IT between development and the help desk regarding timing and nature of changes	M	3	M/L	2	Change advisory committee	
						Not having self-learning to facilitate troubleshooting in the facilities	L	1	H	5		