Internal Controls Policies and Procedures

Rose Hightower

WILEY
John Wiley & Sons, Inc.

Internal Controls Policies and Procedures

Internal Controls Policies and Procedures

Rose Hightower

WILEY
John Wiley & Sons, Inc.

This book is printed on acid-free paper. ♾

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Hightower, Rose.
Internal controls policies and procedures / Rose Hightower.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-28717-0 (paper/website)
1. Auditing, Internal. 2. Corporate governance. 3. Managerial accounting. I. Title.
HF5668.25.H54 2009
657'.458—dc22

2008022105

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

About the Author

Rose Hightower

Rose is an accountant, professor, author and owner of IDÆAL Consulting Solutions International, LLC. She earned an Accounting degree while in Canada and a Master's degree from Syracuse University. Rose has lived and worked in Toronto and New York.

As an energetic, proactive program manager with extensive Fortune 500 experience in identifying and resolving challenges in finance, process management and organizational development. Her career reflects results-oriented leadership with strong creative problem solving and analytical skills. Rose has over 30 years of business experience working with small, medium and corporate clients to improve their efforts and direction in leadership development.

As an accountant, Rose has participated, managed and had oversight responsibilities within various accounting and finance departments including twenty years at IBM, identifying and resolving challenges in finance, process management and organizational assessment.

IDÆAL Consulting Solutions International, LLC a business specializing in redesigning accounting and finance processes, providing tools and skills necessary to improve business operations. The IDÆAL™ philosophy is to provide valued added assessments and transfer skill. Current projects include the design and implementation of documentation programs improving them to address significant accounting deficiencies.

With a life long interest in learning, Rose has taught the mechanics of accounting and finance to college and university students within Canada and the States. Teaching has kept her interest and excitement about the topic fresh and current and combining her real world experience with textbook concepts has provided a additional value to her students.

Rose is the author of Accounting and Finance Policies and Procedures also published by John Wiley and Sons and which serves a prequel and companion to this manual. Within these manuals, she packages current research and proven experience in a ready to use solutions.

You may contact the author by visiting www.idealpolicy.com.

About the Web Site

As a purchaser of this manual, *Accounting and Finance Policies and Procedures*, you have access to the supporting web site: www.wiley.com/go/icpolices

The web site contains everything within the book. This download is an accumulation of Microsoft Word, Excel, and PowerPoint documents.

The password to enter this site is: controls

Contents

How to use this Manual

Whether you are a large public for-profit corporation or a small independent, there is benefit and value in adopting an internal control program.

This manual is structured as the final product and includes everything you need to document your internal controls program. These documents must be customized and adapted to fit into your company's culture and environment. Throughout the manual there are exercises that, when complete, will assist by providing input to the internal control program and determining your company's internal control posture. Using the URL, www.wiley.com/go/icpolicies download the book and customize it. Follow the document layout and adjust the scope and process flow using your Company's language and procedure. Everything contained within the book is contained within the URL download.

In addition to considering this manual a reference or a "how to," use it as a workbook. As you read through the chapters, perform the exercises to deepen your awareness, identify and prioritize your strategies, and enable employees to be part of the solution. As you review this manual, complete the exercises as you go and you will have a customized internal control program and plan.

In addition to providing some background as to why internal controls are important, this manual includes internal control program-specific policies, procedures, and testing guides—basically everything you need to launch an internal control program. This manual is a companion book to the *Accounting and Finance Policy and Procedure* manual also offered by John Wiley & Sons and available at www.wiley.com/WileyCDA/WileyTitle/productCd-0470259620.html.

This download is an accumulation of Microsoft word, Excel, and PowerPoint documents and Visio charts named and numbered in accordance with the Table of Contents. The downloadable files are distributed on an "as is" basis without warranties.

This download is available for your personal use within your company and must not be further distributed or used for resale. Permission to download the manual is achieved by procuring the book. This book and the downloadable version contain general information and are not intended to address specific circumstances or requirements. The author does not give any warranties, representations, or undertakings, expressed or implied, about the content's quality or fitness for a particular purpose.

For additional program information or support, contact me as the Policyguru via policyguru@idealpolicy.com or visit www.idealpolicy.com.

Preface

To: Chief Financial Officer, Chief Compliance Officer, and Internal Control Program Manager

Do you worry about . . .

- Achieving objectives?
- Being resilient enough to adapt to change in time?
- Managing risks intelligently?
- Recognizing opportunities?

Do you know where your risks are and how to prioritize them? Does your staff have the resources and support they need to recognize and mitigate these risks? Could your company benefit from improved accounting and finance processes?

Having a strong internal control department enables managements to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities and identifying when and where to restructure for future growth.

This manual is brought to internal control, accounting, and finance leaders and professionals who are tasked with implementing a program that will:

- Identify opportunities for effectiveness and efficiencies and reduce risk
- Engage the workforce
- Comply with external governance and reporting requirements such as Securities and Exchange Commission reporting and Sarbanes-Oxley compliance

The Internal Controls department is tasked with a role and responsibility that is more than just governance, risk, and oversight. This manual deals with those topics and presents tools and techniques which can address CEO/CFO worries.

Internal control is more than a role and responsibility; it is a philosophy, culture, and way of thinking. This manual integrates the governance objectives with internal control basics and provides tools and techniques which when applied provide valuable information to the executive leadership and other stakeholders.

As I began researching and preparing this manual, I realized that most large public companies were using and describing the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework in the same way. That is both good and bad news. The good news is that there is considerable evidence and proof that the COSO framework is the generally accepted standard and that there is a consistent look and feel to customized manuals. Internal control program managers become subject matter experts on implementing the framework.

The difficult news for an author is on how to make this subject matter fresh and new. So, although the lists may seem familiar, I hope I bring a fresh, new commonsense approach to applying the framework. Since my strength is in accounting and finance processes and process management, my philosophy is to embed COSO into the very processes we live and work with every day.

Whether you are a large public company or a small independent, the philosophy and approach will add value to your bottom line. The approach is based on laws and regulations and follows a commonsense approach to applying continuous process improvement techniques.

This manual is made up of three parts and includes a discussion of the governance journey, the internal control program, and the internal control testing guides. The manual contains exercises, self-assessments, and various other tools and techniques that can and should be adapted to your control environment.

Many of the concepts presented have been part of the repertoire of the best process-driven companies with the tools and techniques used in other proven models and approaches. This manual brings these concepts together in a fresh way ready for customization and implementation and aimed to achieve bottom-line results. There will be references to Sarbanes-Oxley and COSO; you may recognize the style of self-assessment tools, process management, and project management techniques. These all come together as a road map to implement or refresh your internal control program.

The documents should be used as a starting point for constructing, revitalizing, or documenting your company's internal control program. The program and the testing guides must be personalized and customized to meet your company's needs. Replace my company's (ID*E*AL, LLP; used only at the beginning of some documents) name with your company's name. Follow the document layout and adjust the scope and process flow using your company's language and procedure.

Welcome to an exciting process. As you work through the process, the outcomes will present you with insights and opportunities about your company that you may not be currently aware of. Use this manual as a starting point to assess the maturity of the internal controls program. As you address each of the processes, if the documentation process comes "easily" (i.e., is currently available, is followed by most if not all of your company's subsidiaries and locations; is measured and used as a basis for continuous process improvement) then the process is very mature and there should be no surprises.

Whether you use this manual as a reference, workbook, or guide, congratulations on taking this step and acquiring this valuable resource.

Rose
Rose Hightower
Policyguru@idealpolicy.com
www.idealpolicy.com

GOVERNANCE JOURNEY

BIG G TO LITTLE g GOVERNANCE JOURNEY

Investments in public offerings such as stocks drive the economy. Recent history and current events indicate that stock markets can be unstable for a variety of reasons. In order to protect investors and shareholders, external or public governing organizations have created laws that require companies to provide investors and shareholders with current, accurate, and relevant data and information. Governance is about creating an environment and process for those laws, rules and regulations.

Within this section, there are references to COSO and SOX; if you need a refresher, at the end of this chapter is a summary of these important initiatives.

What is governance? According to the International Federation of Accountants (IFAC), *governance* refers to a set of responsibilities and practices exercised by management with the goal of providing strategic direction and tactical guidance to ensure that company goals and objectives are achieved, risks are identified and managed appropriately, and resources are assigned responsibly. The key message is that governance is a process that, when practiced, reinforces integrity and accountability and demonstrates leadership.

Notice that the definition is not limited to publicly owned companies and is not limited to laws and regulations. There are lessons to be learned from the public companies that have had to deal with the roller coaster impact to their market and asset values. Other "not so public" companies can benefit and reap the bottom line benefits of adopting the tools used on the governance journey. So, if you are a small or private company, there are cautions and benefits that you need to pay attention to.

What is governance about? Governance is about creating and maintaining an ethical work environment, it is about establishing and following the rules; it is about transparency and disclosure. Governance is about creating and following a process to establish, communicate, implement, and measure the principles, rules and regulations required to conduct business.

Where does governance come from? From an accounting and finance point of view, external or big G Governance originates from laws and regulatory organizations such as the Securities and Exchange Commission (SEC), the Financial Accounting Standards Board (FASB) and the Public Company Accounting Oversight Board (PCAOB).

Externally, these governing organizations propose principles, rules and methodologies that are aimed at increasing integrity in the quantitative and qualitative information presented to potential investors and shareholders. To comply with external governance, leaders must find a way to communicate and integrate these externally driven rules and regulations into internal business practices and processes.

Big G Governance originates from sources external to the company while little g governance originates from inside. Some of the forces behind big G Governance include:

- Market stability, which is driven by investors and those in a position of oversight requiring accurate, complete and transparent information
- Political and economic stability which is driven by local governments imposing economic principles and rules on specific industries
- Financial stability which is often identified as the measure between stock prices and asset values

As part of big G Governance, those who are asked to implement the rules are asked to provide input to those regulatory bodies and agencies; for example, public companies satisfy quarterly financial reporting requirements. Those companies and other interested parties provide comments as to current and future direction. The SEC and PCAOB review and evaluate the submissions and comments to ultimately determine the adequacy of current regulation and how these regulations can and must be improved. The SEC and the PCAOB are ultimately responsible for the oversight of compliance with the big G Governance accounting and finance laws and rules.

Compliance with external big G Governance is demonstrated by satisfying reporting requirements and for company leaders to attest to the accuracy and completeness of what is reported. Because the leaders cannot oversee *every* aspect of *every* transaction, leaders translate and integrate the external laws and rules into internal processes, policies and procedures resulting in a little g governance regulatory environment.

The objective of little g governance is simply to integrate big G Governance rules into company processes and comply with reporting and disclosure laws and regulations.

Corporate or little g governance is defined as a process, initiated by the company's board of directors, managers, and other personnel to apply a strategy across the company that will achieve:

- compliance with applicable laws and regulations
- Transparency and reliability of all public reporting and information dispersed for accurate and timely decision making
- Proper (i.e., effective and efficient) functioning of the company's processes, including positive impact on the community; fair and honest dealings with customers, vendors, and employees; compensation; and evaluation of management

Internal or business governance is marked by the review, analysis, and documentation of internal practices and processes required to get work done. Internal business processes define how work is organized and performed; defining the touch points for review, approval and escalation. The business process owners are charged with designing processes that are compliant and yet operate efficiently and effectively.

For our purposes, the term *little g governance* is broadly used to indicate the internal adoption of the external rules and regulations with corporate governance being the bridge between external requirements and expectations and internal processes and resource constraints.

Why governance, why now? It's the law.

Big G and little g governance creation has to be dynamic, that is, it must be able to respond to changing environments with processes incorporating inputs from various constituents, including businesses, investors, creditors, government, and international sources with the purpose of defining and refining governance principles and rules.

For most companies, the focus is on little g governance and the tasks needed to satisfy compliance and oversight regulations. As for any business, there must be identifiable value in the action. The program to establish and oversee little g governance must be about increasing profit contribution to the company through improved process management and decision making.

Little g governance is about creating an internal environment and culture that satisfies internal decision making and external financial reporting. Therefore, while big G Governance is about the law, little g governance is about translating and integrating those laws into the fabric of the business. Little g governance:

- Provides accurate, complete and timely data and information required for informed decision making by customers and other stakeholders

- Provides the workforce with the tools and resources required to act and holding individuals accountable required for a high-performance workforce.
- Leverages the company's core competencies and work systems to manage and improve its key processes. It is about knowing what business you are in and creating an environment to succeed.

Little g governance is about ensuring that operational processes are defined, measured, and reviewed while continuing to achieve the company's goals and objectives and satisfying big G Governance reporting requirements. As part of oversight, operational processes need to be documented and risk assessed to ensure compliance with internal decision making and external reporting.

The journey from Big G to little g governance, to risk and oversight and back to Big G is demonstrated in the following flowchart. Notice that the role and responsibility of little g governance is to implement big G into the operational side of the business and the evaluation and monitoring side with risk/oversight activities. As business areas within the company execute processes, data and information, reports both formal and informal are escalated to the leadership team. The executive leadership and the board of directors are ultimately responsible for the effective and efficient operation of these processes and report the company's outcomes to the big G governance agencies.

Flowcharting the Governance Journey

External regulatory bodies issue directives and guidance. Companies receive and assess these requirements and develop plans to integrate them into their operations or evaluate the risk of not fully implementing them.

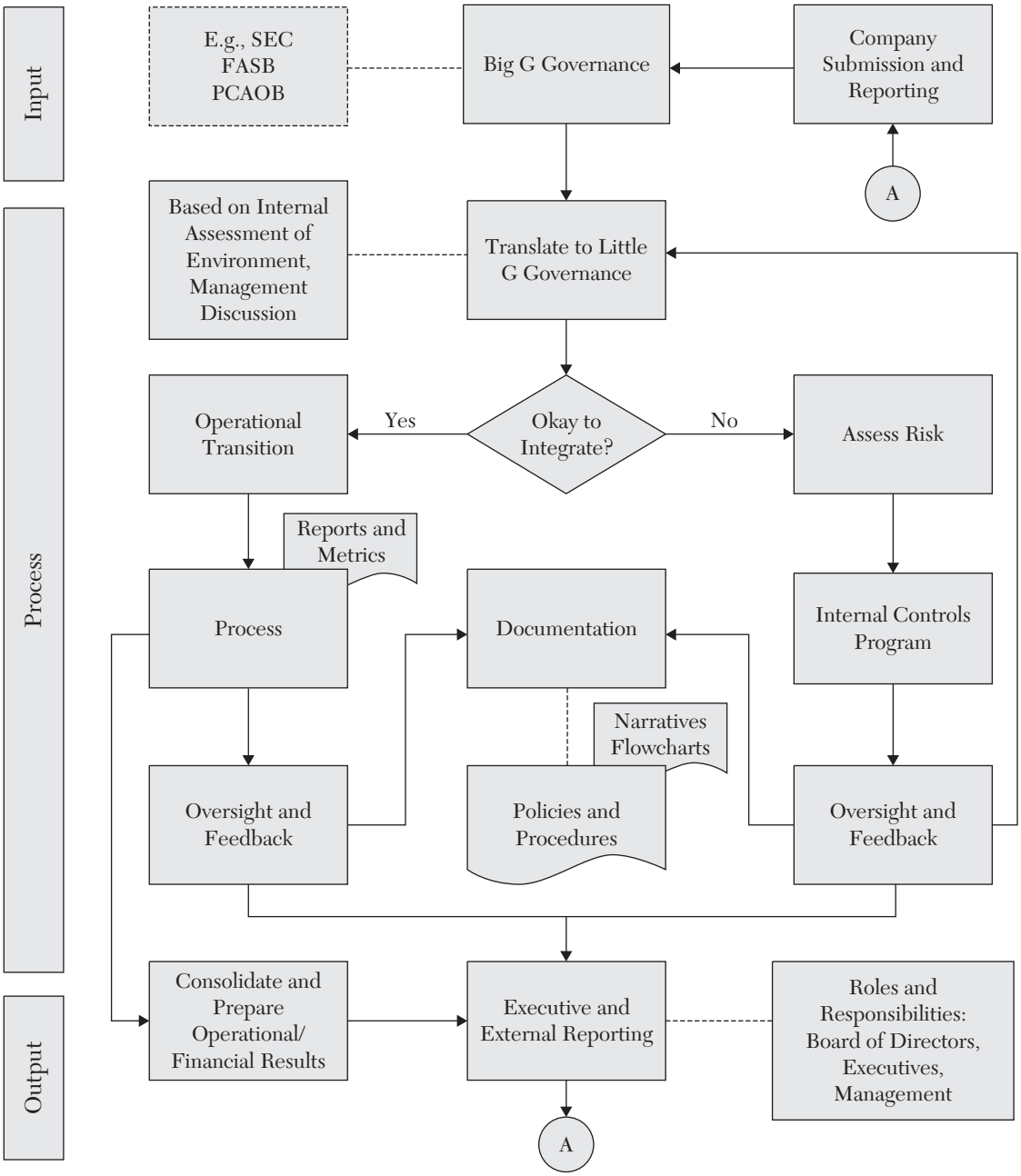
Often, it takes time and resources to respond to the directive, and in the meantime, there is risk. The company needs to assess the requirements and determine where within their operations and to what extent they need to make changes to their processes. This assessment requires understanding and evaluating the company's specific processes and risks. When the company decides where and how to implement process changes, a transition plan and project are initiated and integrated within the operational side of the business. During the transition period and thereafter there may be remaining risk to the company that requires monitoring and periodic reassessment.

Once implemented and deployed, processes are updated and the impact of the change in regulation is measured via the processing of transactions. The effectiveness and efficiency of the operational processes is overseen by programs that measure risk and compliance.

The company uses risk assessment techniques to assess the risk of not conforming or not fully conforming. If the decision is to not accept the risk, then operational processes are updated. If the decision is to accept a level of risk, then the risk needs to be managed with oversight built into the risk management process.

With the results of operational processes confirmed, and the impact and effect of risks identified, reports are issued to executive leadership and the board of directors. Once approved, they release external reports to satisfy external regulatory reporting requirements.

Additions, deletions and changes to the external rules and regulations occur as the external regulatory bodies receive company reports and feedback and as those agencies evaluate other economic environmental indicators. The governance journey is complete.


Input
Process
Output
E.g., SEC
FASB
PCAOB
Big G Governance
Company
Submission and
Reporting
A
Based on Internal
Assessment of
Environment,
Management
Discussion
Translate to Little
G Governance
Operational
Transition
Yes
Okay to
Integrate?
No
Assess Risk
Reports and
Metrics
Process
Documentation
Internal Controls
Program
Narratives
Flowcharts
Oversight and
Feedback
Policies and
Procedures
Oversight and
Feedback
Consolidate and
Prepare
Operational/
Financial Results
Executive and
External Reporting
Roles and
Responsibilities:
Board of Directors,
Executives,
Management
A

APPENDIX

SOME BACKGROUND INFORMATION ON COSO, SOX AND PCAOB

Every internal control manual today, refers to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework and the Sarbanes-Oxley Act (SOX). For those not familiar with these initiatives, following is a brief overview and positioning of these important milestones as they relate to the internal control governance journey.

COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1992 issued *Internal Control–Integrated Framework* to help businesses and other entities assess and enhance their internal control systems. This framework has been recognized by executives, board members, regulators, standard setters, professional organizations, and others as an appropriate comprehensive Framework for Internal Controls. For further information on COSO go to www.coso.org.

This book neither replaces nor modifies the framework, but rather provides guidance on how to integrate it within your internal control environment. Volumes have been written to discuss and describe the COSO concepts; rather than emphasizing COSO, this manual uses COSO as a tool and guide to implement your customized program. The internal control process begins with management's setting financial reporting objectives relevant to the company's particular business activities and circumstances.

Once set, management identifies and assesses a variety of risks to those objectives, determines which risks could result in a material misstatement in financial reporting and determines how the risks should be managed through a range of control activities. Management implements approaches to capture process and communicate information needed for financial reporting and other components of the internal control system. All this is done in context to the company's control environment, which is shaped and refined as necessary to provide the appropriate tone from the top. These components are monitored to help ensure that controls continue to operate properly over time.

The COSO components include:

- *Control Environment* which is an indicator of the level of control consciousness of the company. It is the basis for all the other components providing direction, discipline, and structure.
- *Risk Assessment* represents the identification and analysis of relevant risks to achieving objectives. This component forms the basis for how risks should be identified, managed, and reported.
- *Control Activities* are embedded in the operational and financial processes and ensure that necessary actions are taken.
- *Information and Communication* identifies, captures, and communicates upstream and downstream data and information.
- *Monitor* refers to the process that assesses and evaluates process effectiveness, efficiency and compliance in addressing the internal control objectives. Included within the monitor component of COSO is the responsibility to report on the company's internal control posture.

Monitoring Challenges in Attaining Cost-Effective Internal Controls

This particularly is the case where managers view control as an administrative burden to be added onto existing business systems, rather than recognizing the business need and benefit for effective internal control that is integrated with core processes. Among the challenges are:

- Obtaining sufficient resources to achieve adequate segregation of duties
- Management's ability to dominate activities with significant opportunities for management override control
- Recruiting individuals with requisite financial reporting and other expertise to serve effectively on the board of directors and audit committees
- Recruiting and retaining personnel with sufficient experience and skill in accounting and financial reporting
- Taking management attention from running the business in order to provide sufficient focus on accounting and financial reporting
- Maintaining appropriate control over computer information systems with limited technical resources

The COSO framework recognizes that an entity must first have in place an appropriate set of financial reporting objectives. At a high level, the objective of financial reporting is to prepare reliable financial statements, which involves attaining reasonable assurance that the financial statements are free from material misstatement. Flowing from this high-level objective, management establishes supporting objectives related to the company's business activities and circumstances and their proper reflection in the company's financial statement accounts and related disclosures. Efficiencies are gained by focusing on only those objectives directly applicable to the business and related to its activities and circumstances that are material to the financial statements.

Sarbanes-Oxley

The Public Accounting Reform and Investor Protection Act of 2002 is commonly referred to as the Sarbanes-Oxley Act, named after its sponsors, U.S. Senator Paul Sarbanes and U.S. Representative Michael Oxley. The Sarbanes-Oxley Act (SOX) requires that all public companies do something that they probably should have been doing all along: assign the chief executive officer (CEO) and the chief financial officer (CFO) authority over the company's internal controls and the opportunity to demonstrate competent and transparent governance.

The major sections of SOX that affect this topic include:

- Section 301, which relates to accounting and auditing complaints
- Section 302, which addresses disclosure procedures and controls, including the quarterly CEO/CFO certification
- Section 404, which addresses internal controls over financial reporting certification and attestation
- Section 409, which requires the rapid disclosure of material events

SOX requirements are based on fundamental principles of good business. Every business whether required to comply with SOX or not, benefits from implementing and paying attention to internal controls. The benefits of a strong internal control structure and program are that it delivers business value far beyond the mandatory compliance with SOX regulations. There are two sections within SOX that require mention here: sections 302 and 404.

Section 302 focuses on management's responsibility. CEOs and CFOs must personally certify that they are responsible for disclosure controls and procedures. Each quarterly filing must contain an evaluation of the design and effectiveness of these controls.

Section 404 mandates an annual evaluation of the company's internal controls program. The rule requires management to base its evaluation on a recognized framework such as COSO. Executive management is directed to support its evaluation with sufficient evidence, including documentation. Section 404 additionally places responsibilities on the external auditors, who must audit management's assessment and issue a related audit opinion.

Together, SOX and COSO have provided the mandate and defined the approach that internal control departments are to use. Companies that focus merely on legal compliance with the act will miss the potential benefits of using the act's provisions as a catalyst for company-wide change. Companies can leverage the SOX provisions to improve employee efficiency and productivity, streamline operations, and make better financial decisions through timelier, more transparent financial information. The act represents an opportunity to elevate corporate integrity, restore investor confidence, and move the economy forward.

There is additional information on the Sarbanes-Oxley Act and how it is integrated within the internal control program in the chapter "Quarterly Subcertification Program." For additional information on the Sarbanes-Oxley Act, go to www.sec.gov/about/laws/soa2002.pdf.

PCAOB

The Public Company Accounting Oversight Board (PCAOB) receives its mandate from section 102 of the Sarbanes-Oxley Act of 2002, which requires accounting firms to be registered with the board if they prepare or issue audit reports on U.S. public companies.

The PCAOB is a private-sector nonprofit organization created by SOX to oversee the auditors of public companies to order to protect the interests of investors and further the public interest in the preparation of informative, fair and independent audit reports.

The PCAOB audits the auditors and provides reports to the public. The PCAOB is mandated to provide, communicate and test compliance with generally accepted auditing standards. Additional information for the PCAOB can be found at http://www.pcaobus.org/.

RISK ASSESSMENT

We live in unstable and volatile times, where a company's ability to conduct business or its very life can be denied by forces seemingly outside its control. There seems to be a never-ending list of factors that require a company to always be diligent. These factors include but are not limited to impacts from events that involve:

- Corruption, fraud
- Economic cycles
- Globalization
- Increasing regulation
- Litigation
- Piracy of intellectual property
- Natural disasters
- Supply chain constraints, restraints
- Geopolitical unrest
- Competitive or industry consolidation
- Consumer demand
- Cyber crime

Assessing or not assessing these risks brings its own price tag in the form of missed opportunities, information and program overload, growing risk aversion and a high cost for failure. The result is a renewed scope and focus for risk, including the company's preparedness for recognizing and managing risk when it presents itself.

Well-run and successful companies know how to use risk to their advantage. Within their organization they have those who monitor and even seek risky opportunities with the purpose of driving innovation and seeking commercial advantage. These same companies also know that resources are drained and wasted when there are inappropriate levels of risk. Understanding the difference is vital.

Innovation and thrill-seeking opportunities may become the domain of sales, marketing, and research and development. There is disproportionate financial risk when innovation and thrill-seeking are not aligned with the company's long-term goals and objectives or when appropriate levels of due financial, technical and operational diligence are not performed *before* investment in these pursuits occurs.

Operational risk occurs when there are unacceptable levels of waste identified by effectiveness and efficiency measures. Financial risk presents itself when budget or plan objectives are not met and when there are gaps within internal control procedure that indicate an opportunity for fraud or misuse may occur.

Our focus in this manual is on the type of risk that compromises your internal controls posture. This includes operational and financial risk.

What is risk? Risk is about being prepared for the unexpected; whether fortuitous or perilous. Risk is about anticipating what is not planned and being confident and able to apply critical thinking faster than the competition. Risk management involves a process of planning, organizing, leading, controlling, and communicating in order to minimize the effects of risk on an organization's capital and earnings.

Using a total company or total enterprise view, management expands the depth and breadth of processes to include not just risks associated with accidental losses but also with financial, strategic and operational situations.

What is risk about? Risk is about understanding its nature and adopting a respectful watchful approach. Companies that understand risk and its place in running a business use it to mitigate unnecessary threats and may even be able to win and make money by taking intelligent risks. Risk management adds value to the bottom line when it provides opportunities for cost savings through identifying and correcting operational inefficiencies, when it promotes "out of the box" thinking, when it opens opportunities to leapfrog the competition. Risk is about being confident and prepared for action.

Not all risk needs to be avoided. For instance, refer back to the Governance flowchart. When big G Governance rules and regulations are received, an assessment needs to be conducted to determine what, if any process is affected. Once the affected processes are identified analysis is required to determine the best approach to comply with the regulation including a cost-versus-benefit analysis. The decision may be to:

- Accept the regulation and integrate it within the current process
- Accept the regulation and integrate it within a redesigned process developing a transition process plan
- Accept the regulation and determine a top level management approach to meet the regulatory reporting requirements and not integrate it within the process
- Partially accept the regulation and integrate it within the current or redesigned process. The part of the regulation not adopted is also considered risk and must be managed. Those areas not adopted must be fully documented including rationale as to why it cannot be adopted at this time. Where possible, mitigating controls must be adopted and monitored collecting evidence to demonstrate a "good faith" effort when regulators call on the company. Even with documentation and mitigating controls, regulators may still consider anything less than full adoption a nonconformation to the law. Consider the cost of potential penalties and risk to the company's reputation if nonconformance is the decision.

Why risk management, why now? It's the environment we live and work in.

Opportunities for risk permeate every aspect of the organization including those points where the external environment imposes specific constraints and/or demands specific information. The following table lists and describes the various types of risks we, as accounting and finance professionals often encounter.

Type of Risk	Description
Business continuity	Assurance that systems and business activities are redundant and recoverable in the event of natural disaster or operational failure.
Business environment and governance	Is an indicator of the company's culture; sets the tone of the organization, business unit, or function; influences the control consciousness of its people; and is the foundation of risk management and internal control, providing discipline and structure.
Change management	Company leaders and employees are unable or unwilling to implement process / product / service improvements quickly enough to keep pace with the changing marketplace.
Compliance	A measure of conformity with applicable laws and regulations, as well as internal policies and procedures.
Customer satisfaction/reputation	The risk that the company's goods and/or services do not consistently meet or exceed customer expectations because of lack of focus on customer needs.
Data security	The protection and safeguarding of sensitive and critical information and the physical assets that support information technology.
Employee health and safety	Health and safety risks are significant due to lack of controls which exposes the company to potentially significant workers' compensation liabilities.
Financial reporting	The risk that financial reports issued to regulatory bodies, existing and prospective investors and lenders include material misstatements or omissions of material facts.

Type of Risk	Description
Human resources	The ability of personnel to effectively manage operating activities, including staff acquisition, staff retention, communication skills, empowerment, accountability, delegation, authority, integrity, judgment, and training.
Legal	Risk that laws and litigation possibilities are not adequately factored into the management decision-making process.
Operational and processing	Ongoing business operations including internal (e.g., culture, people, and process) and external (e.g., competitive, political, and social environment) factors.
Planning	The company's business strategies are not responsible to environmental change, are not driven by appropriate inputs or an effective planning process and are not communicated consistently throughout the organization.
Pricing/contractual commitments	Fluctuations in prices of commodity based materials or products result in a shortfall from budgeted or projected earnings.
Regulatory/industry environment	Regulators impose changes to the industry regulatory environment that result in increased competitive pressures or changes to operational processes.
Reporting	Relates to internal and external reporting and are affected by the preparer's knowledge of generally accepted accounting principles (GAAP), as well as additional regulatory and internal accounting principles.
Risk management	Addresses the company's exposure to loss if market and credit conditions change or if sales, credit, and financing limits are not properly established, updated, or monitored.
Technology	Infrastructure failure (e.g., information systems and telecommunications and/or processing limitations), including failure to properly assess impact of rapidly changing technologies.

Risk and fraud are not the same and fraud deserves a few words. There are generally three requirements for fraud to occur: motivation, opportunity and personality. The degree of motivation is usually dependent on situational pressures and may present itself in the form of a need for money or personal satisfaction or to alleviate a fear of failure. Opportunity refers to having access to a situation where fraud can be perpetrated, such as weaknesses in internal controls, or by necessity or proximity within the operating environment, management styles and corporate culture. Personalities include a personal or behavioral characteristic that demonstrates a willingness to commit fraud. Personal integrity and moral standards need to be "flexible" enough to justify the fraud, perhaps out of a need to feed their children or pay for a family illness.

It is more difficult to mitigate fraud than to mitigate risk. It is difficult to have an effect on an individual's motivation for fraud, since few employees share that level. Personality can sometimes be changed through training and awareness programs. Opportunity is the easiest and most effective requirement to address by developing and implementing effective systems of internal controls. While the occasion for fraud cannot be eliminated, with intelligent supporting programs, the opportunity for it can be diminished by creating an environment of diligence and taking appropriate action at appropriate levels.

Exercise in Evaluating Process Risk

A company's respect for risk shows itself in the company's eagerness for or desire to avoid risk. A company's risk threshold is determined based on the amount of risk exposure or potential adverse impact from an event that the company is willing to accept. As the company reaches its threshold for risk, risk management treatments and business controls are implemented to bring the exposure level back within acceptable levels.

Following is a simple exercise which can be conducted by you or with a select team. Generally the types of things which worry you most attract risk. Without overthinking it, answer the questions with your first impressions, then rate and plot them on the risk matrix.

- Which processes or areas do you think currently have the most risk exposure? Consider using a top-down approach to identify those areas where the highest impact would occur if an internal control weakness was found. Review your financial statements, profit-and-loss statement, and balance sheet. List those accounts that have the largest balances (e.g., revenue, inventory, taxes). It would be helpful to identify what you think the risk might be in these areas.
- Given that you have not conducted any research or investigation, to which of these areas are you prepared to allocate resources? The point being that if these areas worry you and you can name the risk demon and are prepared to spend time and money to find out more; then this is something significant that requires your attention. Consider quantitative as well as qualitative financial and operational impacts for the probability and likelihood that the event will occur.
- What level of risk requires a formal response strategy to mitigate the potentially material impact? In other words, do you want to eliminate all risk, or are you willing to live with certain levels of risk?

Map the risks on the grid according to an impact and probability matrix and group the risks as to those you are willing to:

- *Accept*—retain within the business structure and provide resources to monitor and track
- *Mitigate and control*—establish thresholds and controls to ensure that if pursued the risk will be monitored and tracked and if not pursued a transition plan is established to eliminate it from the business structure
- *Share*—consider alternatives on how the risk may be shared with customers, vendors, suppliers or others
- *Avoid*—eliminate from the business structure and prevent the risk at its source

Risk Matrix