

PCAOB & SEC
Regulatory Expectations:
17 Steps to SOX 302/404 Compliance

White Paper

CAUTION TO READERS

This guide was prepared using information available up to August 31, 2004. It provides general or summary level information about the Sarbanes-Oxley Act of 2002 and related rules, regulations and standards of the U.S. Securities and Exchange Commission, Public Accounting Oversight Board and others. The information presented does not constitute legal advice. Boards of directors, audit committees, companies, external auditors and other readers are encouraged to refer directly to the related laws, regulations and standards and consult with legal counsel concerning their responsibilities.

Paisley Consulting, the leader in business accountability, provides focused solutions on corporate assurance, internal auditing, risk management and compliance. The company's key software offerings include The Paisley Solution, Risk Navigator™, CARD®map, Focus Control Assurance Software®, and AutoAudit®. Services include Collaborative Assurance & Risk Design™ training, Sarbanes-Oxley compliance training courses, and operational risk management training and consulting.

For more information, email sales@paisleyconsulting.com or visit www.paisleyconsulting.com

Tim J. Leech, FCA-CIA, CCSA, CFE Chief Methodology Officer and Principal Consultant

Since joining Paisley Consulting as Principal Consultant, Chief Methodology Officer Tim Leech has been instrumental in the development and implementation of the company's risk and assurance methodology framework. The focus is on providing customers with a set of assurance tools and techniques designed to cost-effectively meet increasingly stringent governance requirements and continuously improve business processes.

With over 25 years of experience working with organizations around the world Tim has earned a reputation as a thought leader. He is responsible for pioneering and delivering the acclaimed Collaborative Assurance & Risk Design™ training system. These CARD® workshops and e-learning modules provide a set of principles and enabling tools that demystify regulatory regimes such as Sarbanes-Oxley, Basel capital accord and, more generally, risk and control assessment. The workshops and modules are custom fit learning aids that help support a client's critical long term risk management and corporate governance needs and better meet rapidly escalating expectations.

Tim was the CEO and founder of CARD® *decisions* Inc., which was acquired by Paisley Consulting in July 2004. Prior to joining Paisley Consulting, Tim's earlier positions included Managing Director of the Canadian subsidiary of Network Security Management Ltd, part of the Hambros Bank group headquartered in London, England, and Director Control and Risk Management Services with Coopers & Lybrand Consulting. Tim also served in a range of internal audit and controllership roles with Gulf Canada in Toronto and Calgary.

An acclaimed international speaker, author and presenter, Tim was elected Fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession. He obtained a bachelor's degree from the University of Toronto, Ontario, and a Master in Business Administration from McMaster University, Hamilton, Ontario. Tim is a member of the Canadian, Alberta and Ontario Institutes of Chartered Accountants and holds a both a Certified Internal Auditor® and Certification in Control Self-Assessment designation from the Institute of Internal Auditors, as well as a Certified Fraud Examiner designation from the Association of Certified Fraud Examiners.

Bruce McCuaig, CA-CIA, CCSA Principal Consultant

In his role as Principal Consultant, Bruce McCuaig is responsible for developing and delivering the Paisley Consulting's proprietary Collaborative Assurance & Risk Design™ training and consulting services. The CARD® training programs are a series of customer-centric, high-energy workshops that deliver leading edge risk and control assessment and design skills to clients. He is also responsible for developing the market for the world's first software product designed to integrate and fully capitalize on the risk and assurance efforts of senior management, work units, internal and external auditors, safety and environmental specialists, compliance units, risk and assurance personnel—CARD® *map*. Since joining Paisley Consulting, Bruce has helped to position the company as a knowledge leader in enterprise governance and risk management solutions.

Previously Bruce held senior executive positions with the Gulf Canada Resources in Calgary and Toronto, and Gulf Oil Corporation in Houston, Texas. While the general auditor of Gulf Canada, he implemented the original work team control self-assessment concepts, including development of officer and board level presentations outlining the benefits of this new approach. Bruce's professional experience includes extensive audit and financial management in the oil and gas industry, both upstream and downstream, as well as exposure to the mining and banking sectors.

Bruce is an experienced speaker, presenter and award winning author, participating regularly in international conferences on the subject of risk and control self-assessment and publishing in professional audit and financial journals. He obtained a degree in business administration from the University of Windsor, Ontario. Bruce is a member of the Canadian Institute of Chartered Accountants and holds a both a Certified Internal Auditor® and Certification in Control Self-Assessment designation from the Institute of Internal Auditors.

Paisley Consulting, the leader in business accountability, provides focused solutions on corporate assurance, internal auditing, risk management and compliance. The company's key software offerings include The Paisley Solution, Risk Navigator™, CARD®*map*, Focus Control Assurance Software®, and AutoAudit®. Services include Collaborative Assurance & Risk Design™ training, Sarbanes-Oxley compliance training courses, and operational risk management training and consulting. For more information, email sales@paisleyconsulting.com or visit www.paisleyconsulting.com

TABLE OF CONTENTS

Caution To Readers.....	i
Section 1: SOX 302 & 404 – The Law	1
Introduction.....	1
Visualizing The Goals Of Sections 302 & 404	2
Linking Section 302 To The 302/404 Overview.....	4
Linking Section 404 To The 302/404 Overview.....	7
SOX 302 & 404 – Regulations & Interpretations.....	8
Regulatory Expectation #1: Prepare Macro Level Anti-Fraud Assessment.....	8
Regulatory Expectation #2: Prepare Macro Level Control Effectiveness Assessments Using A Recognized Control Model (e.g. COSO 1992, COSO ERM 2004, CoCo, Etc)	9
Regulatory Expectation #3: Assess The Effectiveness Of General Computer Controls That Impact On External Financial Disclosures	10
Regulatory Expectation #4: Assess The Effectiveness Of Controls Over The Quarterly And Annual Financial Statement Consolidation And Reporting Processes	11
Regulatory Expectation #5: Define The Locations/Sites To Be Included And The Level/Extent Of Documentation And Testing Required At Each Site	12
Regulatory Expectation #6: Define The General Ledger Accounts, Notes And Supplemental Disclosures That Require Assessment And The Level/Extent Of Documentation And Testing Required For Each Disclosure	12
Regulatory Expectation #7: Define The Processes And Sub-Processes That Impact On The Disclosures Identified In Expectation #6	13
Regulatory Expectation #8: Document Risks, Controls, And Concerns/Residual Risk Information For Each Financial Disclosure	14
Regulatory Expectation #9: Link Risks And Control Documentation To Control Points Identified In MS Visio Or Similar Process Flowchart Documentation Or In Corporate Policies And/Or Procedure Guides.....	18
Regulatory Expectation #10: Assess The Effectiveness Of The Controls In Place/Use For All 10K/Q Account And Note Disclosures.....	19
Regulatory Expectation #11: Determine Whether Any “Significant Deficiencies” Or “Material Weaknesses” Exist In Any Of The Locations/ Accounts /Supplemental Disclosure Processes	21
Regulatory Expectation #12: Evaluate Whether There Are Patterns And/Or Accumulations Of Control Deficiencies That Collectively Indicate A Significant Deficiency Or Material Weakness Exists.....	23
Regulatory Expectation #13: Each Quarter Material Changes In Internal Control Must Be Identified And Assessed.....	24
Regulatory Expectation #14: Assess Control Effectiveness At Third Party Sites When A Service Organization Is Used To Perform Activities/Services That Impact On External Financial Disclosures	26
Regulatory Expectation #15: Management Must Complete Primary Testing/Confirmation Of Key Controls, And Independent Internal Quality Assurance Personnel Must Verify That This Has Been Done.....	27
Regulatory Expectation #16: The Ceo And Cfo Must Take Steps To Ensure Both The Adequacy And Reliability Of The Control Assessment And Verification Work They Rely On To Sign Their Quarterly Section 302 And Annual 404 Control Effectiveness Declarations	28
Regulatory Expectation #17: Meet Sec Document Retention Expectations.....	29

SECTION 1: SOX 302 & 404 – THE LAW

INTRODUCTION

In October of 1987 the Report of the Commission on Fraudulent Financial Reporting, better known as the Treadway Commission report, made the following recommendation:

For the top management of a public company to discharge its obligations to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the financial statements to be fraudulently misstated.

The stated mission of the Treadway Commission was “to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence.”

As a result of the Treadway Commission, the SEC proposed rules in 1988 that bear striking similarities to SOX sections 302 and 404. As a direct result of an aggressive counter lobby from a wide range of interest groups, these proposals were not enacted.

Following the recommendations of the Treadway Commission, the five professional groups in the U.S. that sponsored Treadway developed a control framework titled "Committee of Sponsoring Organizations Internal Control - Integrated Framework" (commonly known as "COSO"). COSO was intended to help public companies, their auditors, advisors, and regulators better understand the key elements of an effective control framework. COSO was released in final in September of 1992.

The dawn of the 21st century brought with it a spate of new disasters that make the governance problems that led to the creation of the Treadway Commission seem trivial in comparison. Massive corporate governance failures at Enron, WorldCom, Adelphia, Allied Irish Bank, HealthSouth and many other large firms shook the confidence of shareholders, lenders, regulators, and the public with respect to the integrity of senior management, competency of boards of directors, integrity of external auditors, lawyers, investment dealers, and others. More generally, it seriously impacted on the confidence of investors in the reliability of external disclosures of listed public companies.

In light of this massive reoccurrence of fraudulent and unreliable financial reporting, U.S. Congress concluded that the few tangible corrective actions that had been taken voluntarily by the private sector since the issuance of the Treadway recommendations in 1987 were not enough. In particular, Congress wanted to redefine a new and more independent auditor/company relationship with significantly more emphasis on the role of the board of directors to oversee and safeguard the reliability of external disclosures and independence of external auditors charged with reporting on those corporate disclosures.

The result of this growing realization was passage of the Sarbanes-Oxley Act in July 2002.

Two of the sections of SOX that pose particularly significant implementation and compliance challenges are sections 302 and 404. Attachment 1 to this paper contains the full text of these two sections.

Simply put, these sections require that the CEO and CFO of an organization certify and assert to stakeholders that SEC disclosures, including the financial statements of the company and all supplemental disclosures, are truthful and reliable, and that management has taken appropriate steps to satisfy themselves that the disclosure processes and controls in the company they oversee are capable of consistently producing financial information stakeholders can rely on (Section 302). The company's external auditor must report on the reliability of management's assessment of internal control (Section 404).

SEC Commissioner Cynthia Glassman summarized the intent of these sections in a speech on September 27, 2002 to the American Society of Corporate Secretaries.

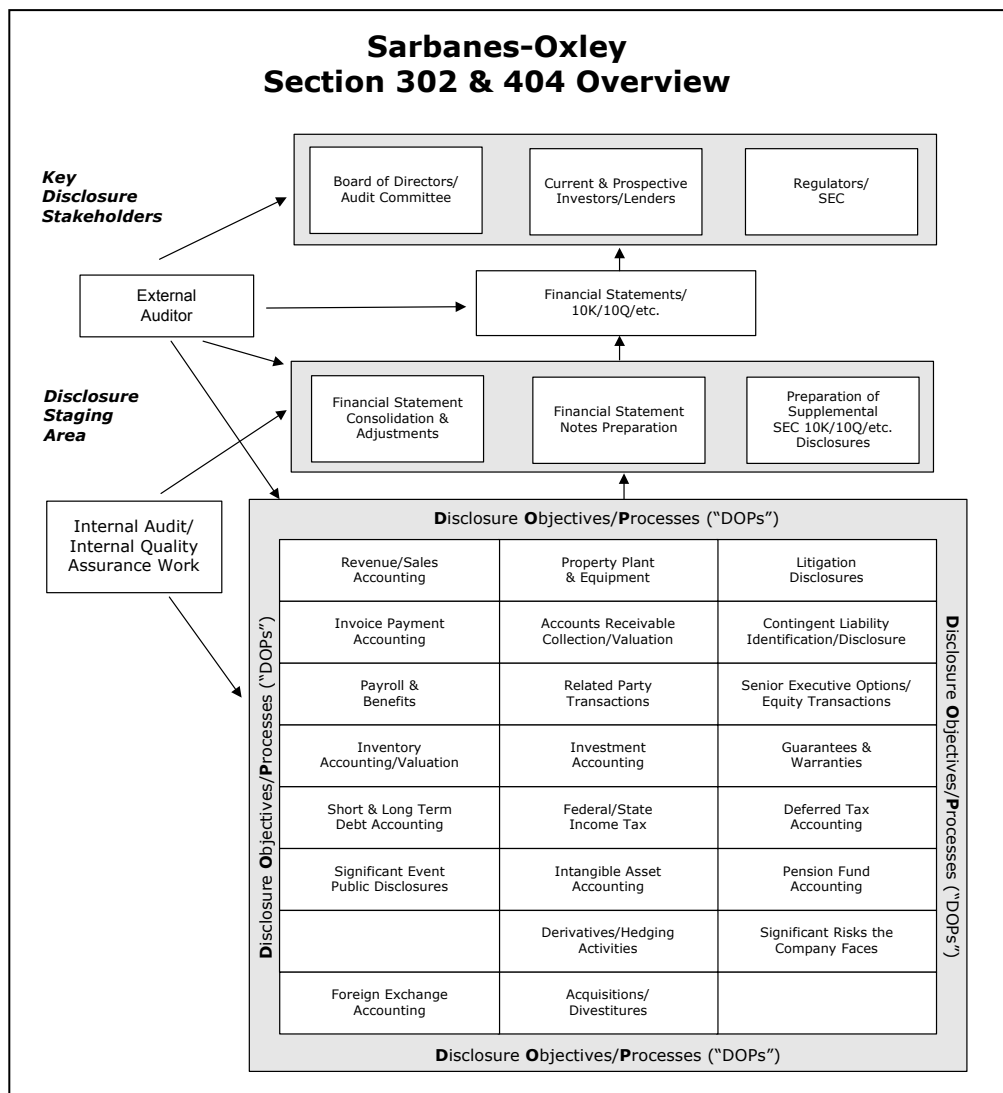
Recognizing that awareness must precede action, Sarbanes-Oxley and the Commission’s rules require the CEO and Board to make certain that procedures are in place to ensure that they hear bad news. Under the Commission’s recently adopted rules, these procedures must ensure that all material information - both financial and non-financial – gets to those responsible for reporting it to the investing public.

This paper demystifies and interprets SOX sections 302 and 404 and provides practical, cost effective suggestions and cautions companies can use to respond to these radical new governance requirements. It is not a legalistic interpretation of the legislation, but rather a common sense rendition of a fairly complex piece of legislation.

VISUALIZING THE GOALS OF SECTIONS 302 & 404

The fundamentals of sections 302 and 404 can be explained using the diagram below. The primary goal of the disclosure system is summarized in the purpose statement of SOX:

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.



For key stakeholders to evaluate any organization, be it a bank, insurance company, oil company, manufacturer, retailer, health care provider, etc., they need reliable information on the history, current financial status and future prospects of the company. Key Disclosure Stakeholders are depicted in the top portion of the overview. The primary goal of the legislation can be stated positively:

Ensure that SEC filings including financial statements, notes, and supplemental disclosures, are reliable.

Primary data sets used by the various disclosure stakeholders are monthly, quarterly, and annual financial statements, notes to the financial statements, and the many supplemental disclosures required by the SEC in 10K and 10Q filings. These data sets can be assembled, consolidated and reported at multiple levels of an organization (i.e. they may be developed in a subsidiary and then roll up to a parent company for consolidation). These activities are depicted simply in the 302/404 Overview as steps that occur in the "Disclosure Staging Area". Staging Area activities have been subdivided in to three core activities:

Financial Statement Consolidation and Adjustments
Financial Statement Notes Preparation
Preparation of Supplemental SEC 10K/10Q/and Other Disclosures

The data necessary to assemble the disclosures comes from a wide range of sources. Illustrative information sources are depicted in the overview as a universe of "Disclosure Objectives/Processes" ("DOPs"). Each DOP has an associated end result objective of timely and reliable disclosure of some sub-set of the company's disclosure package; and a process or system, including internal controls, that support it and manage risks that would cause it to be unreliable. The DOPs depicted in this overview are not exhaustive and will vary depending on the size, complexity and business sector of the organization. Some of the DOPs are highly automated and flow information to the Disclosure Staging Area via sophisticated computer systems. Others are partially automated. A few are done manually and involve significant levels of judgment. The DOPs must deliver generally reliable and complete information to the Disclosure Staging Area for the final consolidated package to be reliable. Some of the DOPs are particularly significant and capable of creating material and dangerous disclosure problems while others are less critical.

Many of the biggest corporate frauds in history have occurred in the Disclosure Staging Area at a level well above the more micro DOP control processes. Highly visible recent examples include Enron, WorldCom, Xerox, and HealthSouth. Particular attention needs to be paid to ensuring there are adequate controls in place to ensure that senior level executives, including CEOs and CFOs, do not improperly force staff to make inappropriate adjustments in the Disclosure Staging Area prior to release to Key Disclosure Stakeholders.

LINKING SECTION 302 TO THE 302/404 OVERVIEW

To focus senior executives on their responsibility for reliable external disclosures Congress enacted SOX section 302. A point-by-point analysis of this section follows.

Section 302 Requirement	Link to the Overview
302(a)(1) the signing officer has reviewed the report	CEO and CFO must review SEC disclosures shipped from the Disclosure Staging Area to Key Disclosure Stakeholders and be able to prove they reviewed it potentially years later.
302(a) (2) based on the officer’s knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;	The CEO and CFO must not allow any SEC disclosures to be shipped to stakeholders from the Disclosure Staging Area with falsehoods or omissions. The "omit to state" portion of this section means that the CEO and CFO must take steps to ensure that the flow from the DOPs is reliable and complete.
302(a)(3)based on such officer’s knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;	This requirement suggests that the disclosures to key stakeholders must be more than just being in compliance with generally accepted U.S. accounting principles - they must “fairly present in all material respects”. This could mean that, in a case like Enron, if the use of Special Purpose Entities caused the statements to not “fairly present in all material respects”, but they were still technically in accordance with U.S. generally accepted accounting principles, this would need to be corrected.
302(a)(4)(A) the signing officers—are responsible for establishing and maintaining internal controls	The CEO and CFO are responsible for setting up and maintaining appropriate and sufficient controls in the Disclosure Staging Area and for the universe of DOPs to ensure timely and reliable external disclosures.
302(a)(4)(B) the signing officers — have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;	The CEO and CFO must be confident that there are adequate controls to ensure that timely and reliable information is flowing to the Disclosure Staging Area related to all key DOPs. For example, if a material lawsuit was launched against the company in a foreign subsidiary, the system must be capable of identifying the situation on a timely basis and feeding the necessary information to the Disclosure Staging Area.

Section 302 Requirement	Link to the Overview
<p>302(a)(4)(C) the signing officers — have evaluated the effectiveness of the issuer’s internal controls as of a date within 90 days prior to the report; and</p>	<p>This is one of the most serious and onerous requirements imposed by SOX. The CEO and CFO are expected to be able to demonstrate that there is a reliable process in place to evaluate, at least quarterly, the controls in place to ensure the reliability of the data being produced by the Disclosure Staging Area and all DOPs. It is important to note that looking at controls in a vacuum without understanding and evaluating the risks that threaten disclosure objectives will produce sub-optimal results and is inconsistent with the principles in the new draft COSO framework scheduled for release in final in Fall 2004. The omission of risk identification and assessment in the assessment process should be considered a significant risk in its own right. Very few companies have formally documented the end result DOPs that support SEC disclosures, the risks to those DOPs, the controls used to mitigate those risks, and current performance data (i.e. the frequency that the Disclosure Staging Area(s) and DOPs produce errors or omissions). The SEC subsequently interpreted this to mean one annual thorough assessment of control effectiveness with an assessment each quarter of any changes that could impact reliable disclosure.</p>
<p>302(a)(5)(A) the signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)----all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer’s ability to record, process, summarize, and report financial data and have identified for the issuer’s auditors any material weaknesses in internal controls; and</p>	<p>The CEO and CFO must be aware of and report to their external auditor and Audit Committee the Disclosure Staging Area(s) and/or DOPs that are producing, or may produce as a result of serious control deficiencies, unreliable and/or incomplete information. It is important to note that the vast majority of companies, at any point in time, have Disclosure Staging Areas and/or some number of DOPs that produce inaccurate or incomplete information. Companies that say they have no control problems should be considered high potential candidates for a corporate governance disaster. Healthy companies recognize, acknowledge, and address the fact there are always control problems - problems that can, but only rarely do, preclude reliable external disclosures.</p>

Section 302 Requirement	Link to the Overview
<p>302(a)(5)(B) the signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) -----any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer’s internal controls; and</p>	<p>This section requires that the CEO and CFO advise the external auditor and audit committee of any situation, regardless of materiality, that indicates dishonesty on the part of any employee that works in a Disclosure Staging Area or plays a significant role in any of the controls that support any of the DOPs that feed the Disclosures Staging Area(s). An example would be if the Controller of a subsidiary is caught falsifying an expense report, putting in an accrual for a liability that had not yet been incurred, or recognizing a sale in the accounts that had not yet been earned. Strictly interpreted, all of these situations would be a reportable item under this section. Depending on how broadly the SEC interprets "employees who have a significant role in the issuer's internal controls", this rule may apply to hundreds of employees that play a significant role in Disclosure Staging Areas, business operations, or any of the DOP control systems.</p>
<p>302(a)(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.</p>	<p>This section requires that in any situation where controls were evaluated at a point in time and subsequently an event occurs that could impact in a significant way on the controls or the reliability of the control processes, this must be documented and reported by the CEO and CFO, including any steps underway to correct it. Presumably, the company must have a system in place capable of scanning the disclosure/risks/ controls universe and detecting significant changes. It isn't clear from the wording whether this is a "to the best of my knowledge" law, with no requirement to positively seek information as to whether changes in the risk/control universe have occurred, or a more onerous expectation that positive steps must be taken by the company to identify significant changes in the control environment.</p>

LINKING SECTION 404 TO THE 302/404 OVERVIEW

Section 404 adds further emphasis to Section 302 by requiring an annual management assessment of controls and an external audit or opinion on its reliability.

Section 404 Requirement	Link to the Overview
<p>S404(a)(1)(2) RULES REQUIRED.</p> <p>The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain an internal control report, which shall—</p> <p>(1) state responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and</p> <p>(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.</p>	<p>This section requires that there be a report that</p> <p>(1) formally acknowledges the responsibility of management for creating and maintaining controls to manage the risks that could cause inaccurate, incomplete or fraudulent data to be shipped from the Disclosure Staging Area(s) or from any of the significant DOPs, and</p> <p>(2) contains an assessment of the reliability of the controls in the Disclosure Staging Area(s) and DOPs to manage risks that could cause, or result in, inaccurate, incomplete and/or fraudulent disclosures being released to key stakeholders.</p> <p>The SEC proposed the content and format of these assertions in the fall of 2002 and will soon be finalizing the specific wording that must be used.</p>
<p>S404(b) INTERNAL CONTROL EVALUATION AND REPORTING.</p> <p>With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.</p>	<p>The external auditor must provide an opinion on the reliability of the assessment developed by management in section 404(a)(2). This requires an audit opinion on the reliability of the management representations on the effectiveness of the controls in the Disclosure Staging Area(s), and controls used to ensure that the DOPs, collectively, generate reliable disclosures for key stakeholders. Although there is a strong bias in the wording, and in many interpretations of the wording, that management will assert that controls are "adequate" or "effective", presumably it would also be acceptable, and much more plausible, if management disclosed in their assessment Disclosure Staging Areas and DOPs that have significant levels of process variability or error rates. The external auditor would then agree or disagree with that assessment much the same way an auditor can give a clean opinion on financial statements that disclose a very bad year in terms of financial results. Once information on process variability/error rate in Disclosure Staging Areas or DOPs is disclosed to the external auditor, the onus would then be on the external auditor to decide if they are still able to give a clean opinion on the financial statements, whether additional work is required by management and/or the external auditor to compensate for the process quality problem from the DOPs and/or Disclosure Staging Areas, or if they are precluded from issuing a "clean report" on the accounts.</p>

SOX 302 & 404 – REGULATIONS & INTERPRETATIONS

REGULATORY EXPECTATION #1: PREPARE MACRO LEVEL ANTI-FRAUD ASSESSMENT

Expectation Guidance

The SEC and PCAOB make it very clear that an assessment of controls designed to prevent and/or detect fraud related activities that could result in unreliable financial disclosures must be completed by management and the company's external auditor.

There are two primary approaches available to do this:

1. Risk Centric Approach: This involves obtaining or developing a list of the fraud related risks that could result in unreliable financial disclosures. Once a list has been prepared, the next step is to link the fraud risks to the control(s) in place to mitigate those risks.

For example, one risk that has emerged is that a company's CFO directs his or her staff to conceal the true financial condition of the company by booking fictitious or inappropriate accounting entries (e.g. allegations in Enron, Parmalat, WorldCom, etc). Control options to mitigate this risk include CFO hiring practices, a code of conduct, a confidential whistle blowing hotline, audit committee oversight and inquiry, an effective internal audit department with responsibility for reliable external financial reporting, competent and independent external audit partners and staff and others. Another risk is that senior executives in head office and/or significant subsidiaries enlist outside suppliers to lie and/or falsify documentation to conceal the true situation from the external auditors. (e.g. Ahold/Foodservices executives allegedly enlisted suppliers to falsify audit confirmations) Control options include confidential whistle blowing hotline, experienced and independent external audit partner and staff, vigilant audit committee, and others. An easy way to approach this task is to develop a database of fraud related losses suffered at other public companies and ask the question "What would stop that fraud related event from happening here?"

2. Control Centric Approach: This involves obtaining or developing a list of the anti-fraud related controls that prevent or detect fraud and assessing whether they are operating. SOX white papers describing disclosure anti-fraud controls that should be in place and the characteristics the controls must have to be considered adequate or effective have been published by a number of public accounting firms and audit associations. (e.g. PricewaterhouseCoopers, Association of Certified Fraud Examiners, AICPA and others) Fraud prevention/detection controls identified should be referenced to the relevant control category/element of the control model used for CEO/CFO SOX 404 assessments. This demonstrates that the control model being referenced in SOX 404 control model representations is actually being used when completing assessments. e.g. COSO 1992 Monitoring, COSO 1992 Risk Assessment, etc.)

When using either method, exceptions identified must be assessed to determine if they are serious enough to be considered a significant deficiency or material weakness and reported. See Regulatory Expectation #11 for more details.

Related References

- Section 302(a)(5)(B)
- SEC section 404 Final Rule section 3(d)
- PCAOB AS#2 paragraph 25
- Article: Distilling SOX 302,404&906 of SOX, Tim J. Leech, Compliance Week May 25, 2004

REGULATORY EXPECTATION #2: PREPARE MACRO LEVEL CONTROL EFFECTIVENESS ASSESSMENTS USING A RECOGNIZED CONTROL MODEL (E.G. COSO 1992, COSO ERM 2004, CoCo, ETC)

Expectation Guidance

This is one of the most difficult SOX 404 requirements. The dominant control model currently in use, COSO 1992, was not developed with the intention that it would be used for pass/fail control effectiveness assessments. Regardless of the practical difficulties this requirement presents, listed public companies that are accelerated filers must start issuing control effectiveness representations referenced to a control model for all year-ends ending after November 15, 2004. (i.e. CEOs and CFOs must state – “XYZ Corporation maintains an effective control system over external financial reporting in accordance with (insert name of control model selected).”

To meet this requirement, users must first select the control model they intend to use for SOX 404 reporting, identify the macro level assessment control criteria included in the model, and then evaluate the degree that the company currently uses or exhibits each of control element and sub-element assessment criteria in that model. For most companies, although other acceptable national control models such as the Canadian CoCo and British Cadbury models are available, this means deciding between COSO 1992 or COSO ERM 2004. Unfortunately, at the current time, very little guidance exists how to evaluate the significance of situations identified during a COSO macro level assessment where the company does not have or exhibit one or more of the control criteria in the control model very well, if at all (i.e. your company doesn't have or do the controls the control model indicates you should have/do).

The good news on a practical level, is that since there is still very little guidance available how to complete this step, it is also very difficult for external auditors, the PCAOB and/or the SEC to identify faults or deficiencies in this aspect of a company's SOX 404 compliance.

Paisley Consulting recommends that companies consider adopting the new COSO ERM (Enterprise Risk Management) framework currently scheduled for release in final in early fall 2004 for macro level control assessment work. The draft of this framework was released for comments in July of 2003. The new COSO ERM framework is better aligned with national and international risk management standards in use in the world, is likely to produce the best business benefits, and is consistent with the approach used in the ISO standard 17799 *Information Technology-Code of practice for information security management*.

Given the significant delays that have occurred issuing the new COSO ERM framework, we are optimistic the authors will include more and better guidance how to complete macro and micro level control assessments using the COSO ERM framework.

In addition to a consolidated company assessment, companies must separately assess significant subsidiaries against the control model selected to determine the degree they conform to the expectations in the control model selected. In cases where some subsidiaries score well against the control model criteria and others do not, companies and their external auditors will have to discuss and agree whether the instances of subsidiary non-compliance with the control model preclude indicating the entire consolidated company maintains an effective control system in accordance with...(insert name of control model).

Related References:

- SEC section 404 Final Rule
- PCAOB AS#2 paragraph 13

- Article: One Strike and Your Out: Distilling Sections 302,404 & 906 of SOX, Tim J. Leech, July issue of Compliance Week

REGULATORY EXPECTATION #3: ASSESS THE EFFECTIVENESS OF GENERAL COMPUTER CONTROLS THAT IMPACT ON EXTERNAL FINANCIAL DISCLOSURES

Expectation Guidance

The importance of assessing the effectiveness of general IT controls that support reliable financial disclosures is emphasized repeatedly in the guidance issued by the SEC and PCAOB. General IT controls relate to:

1. Information technology control environment
2. Program development
3. Program change
4. Access to programs and data
5. Computer operations

These apply to IT general controls for all IT systems including spreadsheet applications that provide information for the 10K and 10Q reports. Controls at third party service providers that provide services that could impact on the company's external disclosures must also be assessed. Examples of these service providers include offshore software development firms, pension fund administrators, payroll services, software application service providers ("ASPs"), outsourced procurement, HR activities and many others. These organizations may, or may not, be retaining outside experts to do SAS 70 Type II or local equivalent internal control reviews (e.g. CICA section 5900 is an example of the Canadian equivalent of a SAS 70 review) to assess and report on the existence and effectiveness of IT general controls and relevant application controls. In some cases, because IT general controls are so critical to the reliability of a company's external disclosures, the SAS 70 reviews that are currently being done at third party sites may not be adequate to meet the SOX 302/404 expectations of external auditors.

Guidance provided by the SEC and PCAOB both indicate that it is important to recognize that companies must covers IT general controls that impact on the integrity of the general ledger and accounting systems and systems that store information used to prepare notes to the financial statements required by GAAP and in supplemental disclosures. This includes information stored in spreadsheet applications such as MS Excel.

The best guidance currently available to help companies complete IT general control reviews is ISO 17799 Information technology – Code of practice for information security management and IT Governance Institute IT CONTROL OBJECTIVES FOR SARBANES-OXLEY. At least one of the major public accounting firms has recently released guidance for assessing controls over spreadsheet applications. (e.g. The Use of Spreadsheets: Considerations for Section for 404 of the Sarbanes-Oxley Act, July 2004, PricewaterhouseCoopers) We expect that over time better, more SOX focused and specific IT controls assessment guidance will emerge.

Companies should first identify the full universe of the IT systems, including those controlled by service providers and internal spreadsheet applications that require assessment and then assign responsibility for creating and maintaining these assessments.

In addition to assessing general IT controls, companies must also consider IT related risks that impact on all individual financial account and note disclosures.

Related References

- SEC section 404 Final Rule
- PCAOB AS#2 paragraphs 40, 50, 53, 73, 75

REGULATORY EXPECTATION #4: ASSESS THE EFFECTIVENESS OF CONTROLS OVER THE QUARTERLY AND ANNUAL FINANCIAL STATEMENT CONSOLIDATION AND REPORTING PROCESSES

Expectation Guidance

Many of the biggest corporate financial statement failures in history can be traced to activities and problems at the highest levels of corporations that occurred during the corporate level accounting adjustment and consolidation process. Some authors refer to this as the assessment of controls over the "period-end reporting process". We refer to it in our technical SOX White Papers and training workshops as assessment of controls in the "disclosure staging area". Important decisions are made in the disclosure staging area on accounting disclosures that involve varying degrees of subjectivity and/or selection of the accounting treatment/approach (e.g. loan loss provision, reserve for inventory obsolescence, impairment of investment values, use of Special Purpose Vehicle entities, etc.).

It is at this stage of the external reporting process that the highest degree of judgment is applied and senior level executives can and, unfortunately, sometimes do, intervene and require staff book inappropriate accounting adjustments. In spite of SOX having been passed in 2002, a May 2004 CFO Magazine survey indicated that nearly half, 47%, of finance employees, were still feeling pressure from their superiors to use aggressive accounting to make results look better.

It is important to note that prior to enactment of SOX, the external disclosure staging area rarely received much attention from Internal Audit departments on the premise that it duplicated the work of external auditors and was therefore inefficient. Audit Committee members rarely asked many questions about the appropriateness of discretionary accounting treatments used by management. This situation has now changed.

The SEC in their SOX 404 final rule has mandated that particular attention be paid to: "controls related to the initiation and processing of non-routine and non-systematic transactions; controls related to the selection and application of appropriate accounting policies;"

Risk and control assessment work needs to address mathematical accuracy, correct application of consolidation rules, selection and application of GAAP, calculation of corporate tax provisions, preparation of supplemental notes and other key activities.

Related References

- SEC SOX 404 Final Rule
- PCAOB AS#2, paragraphs 76-78

REGULATORY EXPECTATION #5: DEFINE THE LOCATIONS/SITES TO BE INCLUDED AND THE LEVEL/EXTENT OF DOCUMENTATION AND TESTING REQUIRED AT EACH SITE

Expectation Guidance

PCAOB Audit Standard #2 (the "Standard") requires that management evaluate and determine which locations should be included as part of their assessment of control effectiveness. The Standard refers to these locations as "individually important" and/or "financially significant". It requires that the external auditor "evaluate their relative financial significance and the risk of material misstatement arising from them". Since management must make the primary control effectiveness assessment prior to the involvement of their external auditor, management should follow the same approach described in Appendix B of the Standard to identify the locations to be covered. Appendix B of PCAOB AS#2 should be referred to for more details on the steps involved.

This step requires evaluation of not only the dollar value of transactions occurring at the location, but also possibility of a significant misstatement and the possible impact on critical performance ratios and indicators used by industry analysts and investors.

As a general rule, this assessment should start by identifying how many different locations/business units maintain a separate general ledger. This universe of locations can then be used as a starting point for the more detailed decisions required by SOX. Once the locations that must be included are identified their materiality to the overall corporate disclosures will dictate the amount of documentation and testing that must be done.

Special attention must be paid to equity method investments, variable interest entities and proportionately consolidated entities. Guidance on the assessment of controls related to investments of this type is available in the PCAOB AS#2 and from the major external audit firms.

Related References

- PCAOB AS#2 paragraph 87 and Appendix B

REGULATORY EXPECTATION #6: DEFINE THE GENERAL LEDGER ACCOUNTS, NOTES AND SUPPLEMENTAL DISCLOSURES THAT REQUIRE ASSESSMENT AND THE LEVEL/EXTENT OF DOCUMENTATION AND TESTING REQUIRED FOR EACH DISCLOSURE

Expectation Guidance

The PCAOB directs auditors to "identify significant account and disclosures, first at the financial statement level and then at the account or disclosure component level.....When identifying significant accounts, the auditor should evaluate both quantitative and qualitative factors." Management should follow the same basic approach in their control assessment work.

The PCAOB goes on to state:

“An account is significant if there is more than a remote likelihood that the account could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement. Other accounts may be significant on a qualitative basis based on the expectations of a reasonable user. For example, investors might be interested in a particular financial statement account even though it is not quantitatively large because it represents an important performance measure.”

In addition to the significant accounting processes, control assessments must also be completed on controls related to information used to prepare notes to the financial statements and supplemental schedules for 10K and 10Q filings.

The PCAOB outlines the approach and amount of testing that the external audit is expected to perform in section 92-107 of the Standard. Management is expected to perform at least as much or more testing than the external auditor is required to perform to come to their conclusion. (e.g. paragraph 41 of PCAOB AS#2 states: *Note: Management cannot use the auditor’s procedures as part of the basis for its assessment of the effectiveness of internal control over financial reporting.*) Some of the major external audit firms have provided more detailed guidance to their clients on the type and amount of testing they expect to see. Since each external audit firm may use a different approach to testing, clients should obtain a copy of this type of guidance when it is available from their external auditor. (e.g. see PwC SOX 404 Practical Guidance for Management July 2004 pages 56-67)

Related References

- PCAOB AS #2 paragraphs 60-67
- PCAOB AS #2 paragraphs 92-107

REGULATORY EXPECTATION #7: DEFINE THE PROCESSES AND SUB-PROCESSES THAT IMPACT ON THE DISCLOSURES IDENTIFIED IN EXPECTATION #6

Expectation Guidance

Once the relevant disclosure objectives, including both account and note disclosures, have been identified and documented, users need to consider the relevant “Financial Statement Assertions” that apply. Assertions are the key attributes of a particular financial disclosure line item or note that must be present in the disclosure. For example, for a Finished Goods Inventory balance relevant assertions include the following:

1. The inventory actually exists. (Existence)
2. The inventory has been correctly valued using the appropriate inventory model according to GAAP such as Last in First Out (“LIFO”), First in First Out (“FIFO”), Moving Average, etc. (Presentation and Disclosure)
3. All inventory owned by the company that should be included in the balance including inventory stored at third party sites has been included. (Completeness)
4. Any third party rights or entitlements have been correctly reflected. (Rights and Obligations)
5. All necessary adjustments for obsolete, damaged or otherwise impaired inventory have been made in the accounts. (Valuation)

These assertions can also be stated as Risks or Threats to the disclosure objective. (e.g. Obsolete inventory has not been identified and appropriate write-down adjustments booked)

In addition to the assertion risks noted above, efforts should be made to identify and rate specific risks to the reliability of all disclosures, both financial statement line items and note disclosures. A risk can be defined as “real or potential situations that could result in the non-achievement of a disclosure objective”.

Once these two steps have been completed, the business processes and specific controls in the processes used to mitigate those risks or threats should be identified and linked to the specific account/note disclosures. Once the related processes are identified they can be documented using narratives or using more structured and formal flowcharting tools such as MS Visio. This process documentation will assist external auditors to complete “walkthroughs” of the processes for each class of transaction and supplemental disclosure.

For processes that support specific disclosures the control points in those processes that address disclosure and assertion risks should be identified and documented.

Users must decide if they will use narrative only documentation of processes, or narrative/text documentation supplemented by flowchart documentation.

An alternative to the sequence described above is to document all processes that impact in any way on external financial disclosures first, complete risk and control assessments on each process, and then later identify and link control points in those processes to specific financial disclosure and assertion risks. This is not a recommended approach since it may result in time and money being spent documenting irrelevant processes and controls that do not play a significant role in ensuring reliable financial disclosures.

Related References

- PCAOB AS#2 paragraphs 68-70
- PCAOB AS#2 paragraphs 71-75
- PCAOB AS#2 paragraph 84

REGULATORY EXPECTATION #8: DOCUMENT RISKS, CONTROLS, AND CONCERNS/RESIDUAL RISK INFORMATION FOR EACH FINANCIAL DISCLOSURE

Expectation Guidance

A number of approach strategies are available to perform the detailed assessment of specific disclosures.

Although the SEC and PCAOB SOX guidance contain only limited references to the need to identify, document and measure risks that could result in unreliable financial disclosures, we believe it is an important step that will receive greater attention in the near future. The focus in SEC and PCAOB guidance issued to date has been on process documentation and control verification/testing.

We believe that a risk-based assessment approach will provide the best overall long-term benefits. This involves identifying the relevant disclosure objectives/accounts (e.g. the accounts, notes and supplemental disclosures to be assessed), identifying and measuring risks that could cause the non-achievement of the disclosure objectives, and then linking those risks to the relevant control points in business processes and elsewhere.

An alternative approach that is used widely and is still acceptable to most external auditors, is to identify the external disclosure account, identify processes that impact on the disclosures, identify

process objectives and the risks that could negatively impact on the process objectives and related controls. Once these steps have been completed, an assessment of control effectiveness and acceptability of the concerns/residual risk status identified in each process can be made.

The new COSO ERM framework scheduled for release in the fall of 2004, IIA professional standards, and risk management standards in many countries around the world all stress the importance of identifying relevant objectives for assessment (in the case of SOX the reliability of accounts, financial statement notes and supplemental disclosures) and then identifying and measuring risks that threaten the achievement of those objectives. After that step has been completed, users can then identify controls in place/use in one or more processes and elsewhere to mitigate those risks.

Risk Identification

To identify and document risks to disclosure objectives/accounts and/or to processes that support those objectives we recommend that a combination of the following methods be utilized:

1. **Research** – For any given objective, business area, or accounting disclosure history provides a rich repository of information on what can go wrong and how it can happen. For SOX assessments, this means that for any given account, financial statement note or supplemental disclosure, guidance on common risks can be obtained from the AICPA, loss event consortiums, the SEC, the press, and other sources via the world-wide-web. An example of this type of resource for a specific industry is the Common Interest Realty Associations Industry Developments ---2003-2004 Audit Risk Alert. This publication promises:

This alert will help you plan and perform your audits by identifying the significant business risks that may result in material misstatement of your client's financial statements.

Many similar guides exist for specific industries and accounting areas. We expect that new and better lists of common risks for the full range of financial disclosure objectives and industry sectors will emerge over time.

The standard assertions risks outlined in paragraph 68 of the PCAOB AS#2 should not be overlooked when developing risk documentation. These include existence or occurrence, completeness, valuation or allocation; rights and obligations; and presentation and disclosure. Paisley Consulting can provide a more detailed list of accounting disclosure assertion risks.

2. **Risk Source Model** – A risk source model is a framework that includes the full range of sources that risks can flow from. The CARD[®] training framework utilizes a 16 risk source framework distilled from leading international risk source frameworks. A number of other risk source models are available. Risk source models can be thought of as a prompt or reference sheet that assists users in recalling the full range of risks that might result in inaccurate or misleading disclosures. A fundamental premise of control assessment is that if you miss identifying or considering a relevant risk to an account or note disclosure there is an excellent chance you won't evaluate the quality of controls in use/place to mitigate that risk. Examples of risk sources in the CARD[®] Risk Source list include customers, suppliers, equipment/technology, human behavior, fraud/corruption, etc.

3. **Loss Event Analysis** – This approach involves systematically identifying situations where a financial disclosure was misstated in the past by the company and then working back to determine the risk or risks that caused the misstatements. This is also known as "cause of failure" approach.

For SOX, a simple and very effective step is to identify the accounts that have historically required adjustments be made at the insistence of the company's external auditor and/or have a history of prior period accounting adjustments to correct errors and misstatements. We recommend 3-5 years of past history be examined to identify problem accounts/note disclosures.

4. **Visualization** – This approach involves imagining situations that would cause an account to be misstated by mentally tracing the evolution of steps or processes that impact on the reliability of the disclosure objective. This can be accomplished by identifying the processes that impact on a

particular disclosure objective, documenting the steps/people involved in the process using narratives and/or flowcharts and tools like MS Visio, and identifying points in the flowchart or narrative where things could go wrong resulting in a misstatement.

A simple example would be "Ensure finished goods inventory balance is reliable and in accordance with GAAP". Related processes include ordering the stock, receiving the stock, moving the stock to a warehouse, releasing stock to production, handling stock returned to the warehouse, etc. As the process of moving stock to the warehouse is visualized, an example of a possible risk would be putting the goods in the wrong bin, silo, etc. which could be later counted and valued incorrectly. This would be particularly likely in situations where different grades exist of what might appear to be the same raw material.

5. Inverse Control Model – This approach involves stating the inverse of the intent of a control category or element as a risk. Examples include the "Risk Assessment" category in the COSO 1992 control model – the inverse to this category is that no one has formally considered risks that would negatively impact on the object and developed/maintained controls to mitigate the risk. Another example is the "Business Objective" category in the draft COSO ERM 2003 framework – the inverse to this category for inventory is that the objective of disclosing reliable inventory numbers has never been formally stated and communicated to the people that need to know and contribute to the achievement of the objective. Stated in common language, the risk to reliable inventory account disclosure is nobody thinks accurate inventory disclosures is their job.

Identifying Controls

There are a number of approaches available to ensure that all relevant controls that support the achievement of a disclosure objective are identified and documented. These include:

1. Use of a control model – This involves selecting a control model and evaluating the degree or extent that elements in the model exist to help ensure the objective being assessed is achieved. If COSO 1992 is used for SOX 404 assessment work this involves identifying controls in all 5 of the primary COSO control categories that exist to help ensure that a specific disclosure objective is achieved. If the more detailed CARD[®] model framework is used, there are 8 categories of controls and up to 10 control sub-elements in each of the 8 categories. Trigger questions exist for each of the CARD[®] model control sub-elements that can be modified to probe for relevant controls to any disclosure objective.

2. Link to risk approach – This involves identifying specific risks to a disclosure objective and then asking what control or controls exist to mitigate each of the risks that have been identified.

An example for inventory account disclosures would be identifying the risk that an inventory part that should be in a shipping box from a supplier has been stolen/removed from the box and the box resealed or it was never in the box in the first place. The next step is to ask what controls or controls would prevent this risk from causing inventory to be misstated. This might include sampling some of the boxes during physical stock counts to ensure they contain what the labeling on the box indicates is in the box, inspecting a sample of boxes when the goods are received from the supplier, and others.

3. Checklist approach – For some disclosure objectives pre-populated lists, sometimes called "ICQs", Internal Control Questionnaires, have been developed for use by assessment teams by external audit firms, internal audit departments or specialty publishers. These lists include questions related to controls that are often relevant to ensuring that a particular disclosure is reliable.

An example for inventory would be an ICQ sheet that asks questions about how physical inventory is taken and whether all the steps one would expect to occur to validate an inventory balance have been executed. A prompt question in an Inventory ICQ would be:

- ✓ "Does someone independent of the primary stock count team independently, without knowing what the primary stock count team determined to be the count, count the stock on a test basis?"

✓ "Are the independent test counts compared to the primary count team results to identify any situations where the primary count team was wrong or inaccurate?"

✓ "Are discrepancies between the primary counts and the independent test counts evaluated to resolve what the true count should be?"

Examples of risks that are linked to these control questions include:

- ✓ the primary count team is careless,
- ✓ the count team consciously misstates inventory counts to conceal a theft,
- ✓ the count team is inadequately trained on how to count/identify/measure stock, etc.

Identifying Concerns / Residual Risk Status

The most common approach to evaluate residual risk (the risk remaining after considering controls in place) is to identify and document situations where one or more of the controls in use or place are found to be missing or deficient (i.e. "control concerns"; "control exceptions"; "audit findings"). The impact of these deficiencies on the company may, or may not, be identified and documented. Although this fairly narrow control effectiveness assessment approach is in widespread use and may be acceptable to some external auditors, we recommend the assessment be expanded to include evaluation of a broader range of residual risk status information. This broader information set helps company management and external auditors come to a well-reasoned assessment of the acceptability of the current situation. Evaluation of residual risk is sometimes referred to as determining an organization or business unit's "risk appetite".

Residual Risk Status includes the following information elements:

1. **Concerns** – These are situations where a risk or threat to an objective has been identified and there is either no control in place to mitigate the risk or the control(s) has/have one or more flaws. Virtually all control assessment approaches in use today include identification of control concerns. Unmitigated or only partially mitigated risk situations are also referred to as control deficiencies, opportunities for improvement, audit findings and other labels. External auditors may, or may not, be satisfied with SOX assessment work if your approach is limited to determining a list of control concerns for evaluation.
2. **Indicator data** – This information is sometimes referred to as "KPIs", Key Performance Indicators, and sometimes more narrowly as "Loss event" data. This is the best available information on how well a specific disclosure objective is currently being achieved.

For SOX, this can include the number of times external auditors have identified and/or insisted on adjustments to specific accounts or notes to the statements, the number of times employees have found errors in accounting disclosures, the number and size of accounting adjustments booked in the current period to correct prior period accounting errors, instances where regulators including the SEC have challenged the appropriateness/ correctness of balances and/disclosures, the number of times customers have found and pointed out accounting errors to the company, the number of prior period account and/or note restatements, etc. This information helps assess whether the errors occurring are anomalies or really do need to be addressed.

3. **Impact data** – this is information about what happens if the disclosure/account is misstated and how bad would/could it be if it was wrong. Not all accounting disclosure mistakes are of equal impact/importance.

For example, does an accounting disclosure effort result in a negative cash impact on the company or only change the accounting period the amount is allocated? Does the stock analyst community and/or SEC focus heavily on the account or financial ratio generated from the account(s)? Will investors be angry if the data was wrong/misstated and punish the company by discounting the stock price? Are there specific criminal, contractual and/or civil penalties that could flow from an account or note

misstatement? (e.g. a disclosure that impacts on a ratio that links to an important debt covenant with a bank) A simple way of stating this is "Some accounting mistakes and misstatements cause more trouble than others."

4. Impediment data – This is information about known situations that are causing an accounting balance to be wrong that are largely outside the control of the responsible business unit(s). In most cases, these impediments have already been brought to the attention of senior management but nothing has been done or very little has been done to correct the situation.

An example might be a weigh scale that is out of calibration or regularly malfunctions that is still used to record inventory shipment receipts, an automated accounting system that has a history of crashing and losing data, an employee that plays an important control role who has a serious drug or alcohol problem, etc.

5. Risk Transfer/Insurance – This is information about contractual indemnities or insurance coverage that could be relevant if a financial disclosure was misstated.

An example is a fixed asset balance related to large and valuable equipment or property the company owns. If there is a fire on December 31 that ruined/destroyed the asset that was not detected/reported, although the fixed asset account would be overstated at the year end there may be a valid and enforceable – "Insurance recovery receivable" (another asset account) that is understated that offsets with the result that the company's overall asset position is generally correct.

Related References

- SEC SOX 404 Final Rule
- COSO ERM 2004 (Scheduled for release in early fall 2004)
- PCAOB AS#2 paragraphs 68-70
- PCAOB AS#2 paragraphs 88-107

REGULATORY EXPECTATION #9: LINK RISKS AND CONTROL DOCUMENTATION TO CONTROL POINTS IDENTIFIED IN MS VISIO OR SIMILAR PROCESS FLOWCHART DOCUMENTATION OR IN CORPORATE POLICIES AND/OR PROCEDURE GUIDES

Expectation Guidance

SEC SOX 404 final rule guidance states:

A company must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the company's internal control over financial reporting. Developing and maintaining such evidential matter is an inherent element of effective internal controls.

A company's assessment of the effectiveness of internal control over financial reporting must be supported by evidential matter, including documentation, regarding both the design of internal controls and the testing processes. This evidential matter should provide reasonable support: for the evaluation of whether the control is designed to prevent or detect material misstatements or omissions; for the conclusion that the tests were appropriately planned and performed; and that the results of the test were appropriately considered. The public accounting firm that is required to attest to, and report on, management's assessment of the effectiveness of the

company's internal control over financial reporting also will require that the company develop and maintain such evidential matter to support management's assessment.

Creation of process mapping flowcharts is one way of meeting the need for control assessment documentation. Narrative descriptions with cross-references where necessary to corporate policies and/or procedure guides is also acceptable. For this documentation to be optimal, the risks that threaten specific disclosures and/or related processes should be linked to the control point(s) identified in the process maps and/or narratives that help mitigate the risks identified and/or be linked to summary narratives of the control point maintained in risk and control assessment software tools.

Because control points identified on process flowcharts are often restricted to direct controls such as comparisons, matching, error correction, edits, etc, users should also identify other relevant controls that play a role in mitigating the disclosure risks such as accountability assignment, commitment controls, risk assessment, performance measurement, monitoring, process oversight and others. Ensuring that all controls, not just the direct controls, are identified is an important step. Companies are expected to be able to demonstrate the use of the control model they are using during their assessment work. Incorrect conclusions on control effectiveness can result if all controls, including relevant compensating controls, are not considered when forming an opinion on the overall effectiveness of controls related to a specific account or note disclosure.

Related References

- PCAOB AS#2 paragraphs 79-82 re walkthroughs
- PCAOB AS#2 paragraphs 123-126 re testing the work of others
- SEC SOX 404 Final Rule – Method of Evaluating

REGULATORY EXPECTATION #10: ASSESS THE EFFECTIVENESS OF THE CONTROLS IN PLACE/USE FOR ALL 10K/Q ACCOUNT AND NOTE DISCLOSURES

Expectation Guidance

There are 5 primary assessment approaches available for use when completing SOX section 302 and 404 assessments. Which approach is used has a major impact on how control effectiveness is assessed. These can be further subdivided in to 5 specialist driven approaches and 5 business unit driven/self-assessment approaches which are then independently quality assured. (i.e. is the assessment done by assurance specialists (internal or external) or by the people responsible for the area) Companies and their advisors are currently using various combinations of these methods to meet their SOX 302/404 responsibilities.

These approaches are:

1. Compliance centric – This approach utilizes a checklist approach that identifies a set of controls that the author(s) of the questionnaire consider relevant to the objective or topic being assessed. Internal auditors and/or business unit personnel evaluate whether the prescribed controls are in use and either confirm they are in use/place, or report the situation as an exception/concern.

How effective this approach is in accurately assessing control effectiveness and ensuring reliable external disclosures is heavily dependent on the quality of the compliance checklist being used and the knowledge and skill of the people using these checklists. A person or group should be formally charged with ensuring that the control checklists used are appropriate and current and that people using them fully understand what they are trying to achieve. It is very difficult to form well-supported and defensible conclusions about the overall effectiveness of controls that support a specific external

disclosure and whether any material weaknesses or significant deficiencies exist using this approach in isolation.

2. Process centric – This approach starts by identifying and documenting processes that impact on external financial disclosures. Although a range of process centric approaches are available, the most common one involves identifying the relevant accounting processes, documenting the disclosure objective(s)/accounts each process supports, identifying risks that threaten the objectives of each process, identifying the controls linked to the risks and then forming a view on the likely effectiveness of those controls collectively and/or individually.

In some cases the sequence used for this approach starts with identification of the account or supplemental disclosure being assessed and then identifying the process or processes that support the disclosure. In other cases all accounting processes in the company are identified and documented and then later linked to the disclosure objective.

The process centric assessment approach came into widespread use in the late 1970s and continues to be very popular with public accounting firms and internal auditors. The attraction for external audit firms is that this approach allows staff to trace accounting transactions from “the cradle to the grave” and better understand how the numbers in the general ledger are generated. We recommend that when this approach is used it be combined with identification of key performance indicators for the accounting disclosure that provide information on the current error rate/mistake rate related to the reliability of the account, note or supplemental disclosures.

3. Objective centric – This approach starts with an end result disclosure objective (for SOX these are related to reliable accounting statement line item disclosures, note disclosures and supplemental disclosures), then identifies and measures risks that could cause the non-achievement of the disclosure objectives, documents the controls in place (including control points in one or more business processes that impact on the disclosure) that help mitigate the risks, and then documents information related to the current residual risk status.

Once those steps are completed, management assesses the overall acceptability of the current residual risk status, the risks that remain after considering controls.

This approach is relatively new and is consistent with the new COSO ERM approach scheduled for release in fall of 2004 and international risk management standards.

4. Risk centric – This approach starts by identifying a context for the assessment. The context could be the whole organization, a sub-unit or a topic. For SOX, an example would be fraud related disclosure errors. The SEC and PCAOB require a macro risk assessment of the controls in place to mitigate fraud related disclosure risks. For the context selected, specific risks that impact on the context are identified and assessed and the controls in place to mitigate those risks identified. For each risk identified, an assessment is made of the controls and the effectiveness of the controls.

5. Control centric – To utilize this approach a user selects a control model or framework for the assessment and then systematically evaluates the degree or extent that the organization and the sub-units use or demonstrate the control elements in the model. For SOX, this means selecting an acceptable control framework for macro control assessment such as COSO 1992, COSO ERM, CoCo, and others, and then assessing the degree or extent the company or a sub-unit conforms to the model. This is a mandatory step to support section 404 representations on the company’s overall control effectiveness in accordance with a specified control model.

For SOX, these 5 approaches are applied as follows:

For SOX section 404 opinions indicating the company has an effective control system at the macro level “in accordance with (*insert control model*)” approach 5 should be used.

To meet the SEC and PCAOB expectations that an anti-fraud assessment be completed, approach 4 is an effective approach, although many external audit firms will also accept approach 1 using an anti-

fraud controls checklist they approve. When the list of prescribed or recommended anti-fraud controls is linked to the control model used for SOX 404 reporting it is a combination of approach 1 and 5.

For IT general controls assessments, different combinations of all 5 assessment approaches can be, and are being, used. ISO standard 17799 – Information Management – Code of practice for information security management is an objective centric approach. COBIT is a mix of the methods described above with a bias to approach 1 since it uses the concept of a “control objective”, an objective to have or use a specified IT control.

To assess controls that support specific financial account and note disclosures the two primary assessment methods in use today are the process centric and objective centric approaches.

For more information on core SOX assessment requirements see the article Distilling SOX 302, 404 and 906 written by Tim Leech that appeared in the May 25, 2004 issue of Compliance Week.

The assessment approaches described above can be used by work unit personnel and verified by independent quality assurance teams, by assurance specialists only, or by work units first with a quality assurance review and testing completed by independent assurance specialists.

Related References:

- PCAOB AS#2 paragraphs 40-46
- PCAOB AS#2 paragraphs 88-107
- SEC SOX 404 Final Rule Method of Evaluating

REGULATORY EXPECTATION #11: DETERMINE WHETHER ANY “SIGNIFICANT DEFICIENCIES” OR “MATERIAL WEAKNESSES” EXIST IN ANY OF THE LOCATIONS/ ACCOUNTS / SUPPLEMENTAL DISCLOSURE PROCESSES

Expectation Guidance

SEC SOX 404 Final Rule guidance indicates that “the term “material weakness” has the same meaning as in the definition under GAAS and attestation standards. The footnote reference in the 404 Final Rule states:

The term “significant deficiency” has the same meaning as the term “reportable condition” as used in AU 325 and AT 501. The terms “material weakness” and “significant deficiency” both represent deficiencies in the design or operation of internal control that could adversely affect a company’s ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements, with a “material weakness” constituting a greater deficiency than a “significant deficiency”. Because of this relationship, it is our judgment that an aggregation of significant deficiencies could constitute a material weakness in a company’s internal control over financial reporting.

PCAOB AS #2 provides definitions for three levels of control deficiencies:

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

*A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is **more than a remote likelihood** that a misstatement of the company's annual or interim **financial statements that is more than inconsequential** will not be prevented or detected.the likelihood of an event is "more than remote" when it is either reasonably possible or probable. A misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements.*

*A material weakness is a significant deficiency, or combination of significant deficiencies, that results in **more than a remote likelihood** that a **material misstatement** of the annual or interim financial statements will not be prevented or detected.*

The SOX legislation and SEC regulations requires that significant deficiencies and material weaknesses must be reported to the company's external auditors and audit committee. The existence of even one material weakness means the company cannot claim in 10Q and 10K filings to have an effective control system and must issue a negative opinion. Specific documented steps must be taken to assess whether collectively, a number of significant deficiencies identified or even a collection of lesser control deficiencies, constitute a material weakness.

In spite of the legalistic tone of these definitions and the attempts to date made by the SEC and PCAOB to provide guidance and examples, it is still very difficult in real life to sort control issues in to these three categories.

A good place to start is to examine the company's previous track record in presenting reliable accounts and note disclosures to their external auditors. We suggest the activity start by assembling and reviewing available information including the following steps:

1. Assemble 3-5 years of historical information of the cases, if any, where the company's external auditor has required adjustments to the accounts or notes. For each instance where this has occurred, an assessment should be made whether there is a significant deficiency or material weakness in the controls related to that account or note disclosure.
2. Review, assemble or create a list of accounting adjustments of "material size" that have been made in the general ledger that relate to prior periods. For each instance where an accounting adjustment has occurred, an assessment should be made whether there is a significant deficiency or material weakness in the controls that allowed inaccurate account and/or note disclosures.
3. If the company has had an internal audit function, 3-5 years of reports and audit findings should be reviewed to determine if any of the issues that relate to, or could impact on, the reliability of accounting disclosures remain uncorrected that may qualify as a significant deficiency or material weakness. Internal audit should also be required to report control issues they identify related to financial disclosure systems using the SEC/PCAOB Material Weakness/Significant Deficiency rating system.
4. If the company's external auditor has issued management letters detailing concerns with the company's controls and/or control environment, 3-5 years of these should be reviewed to determine if any of the issues that remain uncorrected qualify as a significant deficiency or material weakness.

For each of the recommended steps above, the steps taken and results produced should be documented and the decisions arrived at on control deficiency classification maintained on file.

In addition to the review of known information about control deficiencies the company must complete the steps outlined in earlier Regulatory Expectation guidance including:

- An assessment of the company's anti-fraud controls.
- An assessment of the company's conformance to the control model used for SOX 404 reporting including an assessment of effectiveness of the company's audit committee.
- An assessment of the IT general control for all computer applications that provide information for the company's 10K and 10Q filings.
- An assessment of the controls for the specific accounting, notes and supplemental disclosures.

The PCAOB AS#2 indicates quite clearly that the existence of any of the following is a significant deficiency and a "strong indicator" that a material weakness exists:

1. Restatement of previously issued financial statements.
2. Identification of a material misstatement in draft financial statements in the current period not identified by management.
3. Weak audit committee oversight.
4. Ineffective internal audit function.
5. For large organizations an ineffective compliance group.
6. Identification of fraud of any magnitude on the part of senior management.
7. Significant control deficiencies that have been communicated to senior management that remain uncorrected after some reasonable period of time.

Related References

- SEC SOX 404 Final Rule Material Weakness in the Internal Control Over Financial Reporting
- PCAOB AS#2 paragraphs 9 and 10
- PCAOB AS#2 paragraphs 130-141
- PACAOB AS#2 Appendix D

REGULATORY EXPECTATION #12: EVALUATE WHETHER THERE ARE PATTERNS AND/OR ACCUMULATIONS OF CONTROL DEFICIENCIES THAT COLLECTIVELY INDICATE A SIGNIFICANT DEFICIENCY OR MATERIAL WEAKNESS EXISTS

Expectation Guidance

PCAOB AS#2 provides the following guidance for external auditors:

The auditor must evaluate identified control deficiencies and determine whether the deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

Since this is the guidance that external auditors must follow it is also applicable to the control effectiveness assessments made by management.

In addition to the earlier guidance on how to identify individual instances of significant deficiencies and material weaknesses, this step stipulates that senior management must examine the entire universe of control deficiencies that have been identified across the company, the group, and even around the world in the case of large multi-nationals, to determine whether individually insignificant control deficiencies collectively constitute a significant deficiency or material weakness.

Although there is very little authoritative guidance on how this should be done, the following steps are recommended:

1. Carefully examine the results of the assessment of the company's controls relative to the control model selected for SOX 404 reporting. Major deficiencies in specific control categories and sub-categories, particularly controls related to monitoring and oversight, should be considered particularly problematic. Other areas that warrant serious attention are problems with commitment controls and performance measurement related to reliable external disclosures.
2. Examine patterns in disclosure errors that have been identified in past periods. If trends are emerging of repeat disclosure errors, and it appears little or no corrective action likely to rectify the situation is underway, this should be a warning flag.
3. Review the overall strength and competency of the CFO/Controller's organization. High turnover, crisis management, weak explanations of account movements, inadequate explanations of significant budget to actual differences, a history of problems with tax authorities, a history of high involvement of external auditors to calculate tax provisions, select the company's accounting treatments and handle complicated accounting issues are all warning signs of a possible material weakness in the company's control system.
(Note: External audit firms that have historically played a major role determining tax provisions, writing note disclosures, or selecting GAAP, should carefully evaluate whether they can form an opinion on the controls that support accounting and note disclosures.)
4. If Internal Audit still reports administratively to the CFO and/or has been discouraged or forbidden in the past from reviewing controls over the external accounting disclosure process, be aware that in the post-SOX era this may be indicative of a pattern of behavior that collectively constitutes a material weakness.
5. Carefully assess the design of the company's reward system to determine if it puts too much pressure on accounting personnel and individual business units to "cook the books". Be particularly alert if the reward structure for the CFO and Controller is heavily linked to stock options and achievement of short-term performance targets.

Related References

- PCAOB AS #2 paragraphs 127-141

REGULATORY EXPECTATION #13: EACH QUARTER MATERIAL CHANGES IN INTERNAL CONTROL MUST BE IDENTIFIED AND ASSESSED

Expectation Guidance

Section 302(a)(4)(C) stipulates that:

"the signing officers – have evaluated the effectiveness of an issuer's internal controls as of a date within 90 days prior to the report"

This section, as originally passed by U.S. Congress, implied that a full assessment of controls had to be completed four times a year.

The SEC in the Final Rule guidance for Section 404 concluded that a full reassessment of disclosure controls four times a year would be too onerous for registrants.

The SEC concluded in SOX 404 Final Rule:

After consideration of the comments received, we have decided not to require quarterly evaluations of internal control over financial reporting that are as extensive as the annual evaluation.

Accordingly, we are adopting amendments that require a company's management, with the participation of the principal executive and financial officers, to evaluate any change in the company's internal control over financial reporting that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting. We have also adopted a modification to the Section 302 certification requirement and our disclosure requirements to adopt this approach as discussed below.

....While the evaluation is of effectiveness overall, a company's management has the ability to make judgments (and is responsible for its judgments) that evaluations, particularly quarterly evaluations, should focus on developments since the most recent evaluation, areas of weakness or continuing concern or other aspects of disclosure controls and procedures that merit attention.

What the SEC now expects is a re-evaluation of each disclosure control assessment to identify any changes that may have occurred in the risks to all disclosure objectives, either in terms of likelihood and/or consequence and/or the controls in place to mitigate those risks. They also imply that there should be a careful evaluation of progress being made to correct outstanding control deficiencies. Although the rules do not explicitly suggest it, we also believe that consideration should be given to residual risk status information that suggests or indicates changes in the risks to specific disclosure and/or the actual or perceived effectiveness of controls, specifically information that indicates changes to disclosure objective error rates. (i.e. the number of disclosures issued that are later proven to have some error component)

This is any information on the number of disclosure process/control failures that have become known. An example would be that during the quarter a number of customers objected to invoices sent to them because they didn't receive the goods or customers called asking when an invoice was going to be issued for goods they already have received. Both are examples of "Key Performance Indicators" with respect to the disclosure objectives of reliable sales and reliable accounts receivable.

Related References

- SEC Final Rule Re SOX Section 404: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

REGULATORY EXPECTATION #14: ASSESS CONTROL EFFECTIVENESS AT THIRD PARTY SITES WHEN A SERVICE ORGANIZATION IS USED TO PERFORM ACTIVITIES/SERVICES THAT IMPACT ON EXTERNAL FINANCIAL DISCLOSURES

Expectation Guidance

Many organizations use a variety of service providers to handle and administer activities that have or could have a material impact on the company's financial statement and note disclosures. This can range from outsourced Human Resource management, payroll, pension fund administration, software development, software hosting, calculation of actuarial reserves and many other activities.

The first task is to carefully inventory all service providers that provide any services that could have a material impact on financial statement disclosures and determine whether SAS 70 Type II control reviews or equivalent are being performed (i.e. an independent assessment of controls). Procedures to be followed will vary depending on the existence of a SAS 70 Type II report or equivalent.

The SEC in a June 2004 release responding to frequently asked questions stated:

In a situation where management has outsourced certain functions to third part service provider(s), management maintains a responsibility to assess controls over the outsourced operations. However, management would be able to rely on the Type 2 SAS 70 report even if the auditors for both companies were the same. On the other hand, if management were to engage the registrant's audit firm to also prepare the Type 2 SAS 70 report on the service organization, management would not be able to rely on that report for purposes of assessing internal control over financial reporting. Management would be able to rely on a Type 2 SAS 70 report on the service provider that is as of a different year-end. Note, however, that management is still responsible for maintaining and evaluating, as appropriate, controls over the flow of information to and from the service organization.

As a general statement, this area still continues to be very problematic in spite of the SEC attempt at clarification above. On the one hand the SEC makes it clear that management retains final responsibility for internal control effectiveness representations. On the other hand they appear to indicate reliance on a SAS 70 Type II report is adequate. In light of the fact that the process to generate SAS 70 Type II reports is generally significantly less rigorous than the steps required to be completed on control activities that impact on the financial statements done in-house, this would appear to represent inconsistent logic.

At the current time, management of outsourced service providers do not have to complete and maintain rigorous self-assessment risk and control assessment documentation to obtain a "clean" or unqualified SAS 70 Type II report nor do they have to scan their entire environment quarterly to assess whether significant changes have occurred. (SOX section 302) SAS 70 reviews do not require the auditor to assess and report on the quality of control self-assessment work done at these organizations.

It is very likely that some organizations have such significant reliance on service providers that they will have to negotiate significantly more rigorous standards and procedures that go beyond current SAS 70 expectations to meet the overall intent of SOX section 404.

In light of the complexity and approach inconsistencies in this area we recommend that clients consult their professional advisors and the references noted below to address this area.

Related References

- PCAOB AS#2 paragraph 41
- SEC SOX 404 Frequently Asked Questions June 2004 Question 14
- PCAOB Staff Questions and Answers , SOX 404 June 23, 2004 Questions 24, 25 and 26
- Sarbanes-Oxley Act: Section 404 Practical Guidance for Management, July 2004
PricewaterhouseCoopers, Section IV: Use of Service Organizations

(NOTE: We strongly recommend company's contact their own external audit firm to obtain a written interpretation of the rules and expectations in this area.)

REGULATORY EXPECTATION #15: MANAGEMENT MUST COMPLETE PRIMARY TESTING/CONFIRMATION OF KEY CONTROLS, AND INDEPENDENT INTERNAL QUALITY ASSURANCE PERSONNEL MUST VERIFY THAT THIS HAS BEEN DONE

Expectation Guidance

This area presents major challenges to management because of the significant amount of judgment involved in determining what are the "key controls". Historically auditors have concentrated primarily on what is classified as direct control activities in COSO. Although these controls were sometimes deficient or absent in major corporate failures, they were rarely the "key controls" that allowed major problems to happen and continue undetected for some period of time.

The SEC in SOX 404 final rule under the caption "Method of Evaluating" states:

An assessment of the effectiveness of internal control over financial reporting must be supported by evidential matter, including documentation, regarding both the design of internal controls and the testing processes. This evidential matter should provide reasonable support: for the evaluation of whether the control is designed to prevent or detect material misstatement or omissions; for the conclusion that the tests were appropriately planned and performed; and that the tests were appropriately considered. The public accounting firm that is required to attest to, and report on, management's assessment of the effectiveness of the company's internal control over financial reporting will require that the company develop and maintain such evidential matter to support management's assessment.

The PCAOB directs external auditors to determine whether management has addressed the following elements:

**Determining which controls should be tested, including controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include:*

- *Controls over initiating, authorizing, recording, processing, and reporting significant accounts and disclosures and related assertions embodied in the financial statements.*
- *Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles.*
- *Antifraud programs and controls.*

- *Controls, including information technology general controls, on which other controls are dependent.*
- *Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates.*
- *Company level controls (as described in paragraph 53) including: - the control environment and controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, authorize, record and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (for example, consolidating adjustments, report combinations, and reclassifications).*

At a minimum, companies need to ensure that the controls related to these issues are covered.

In addition to giving special attention to the areas identified above, management should apply a risk based approach to develop their testing strategy that starts by identifying the most significant risks that threaten the reliability of external disclosures at the macro, mid and individual disclosure levels. Once these risks are identified, the controls that play a key role mitigating these risks should be identified, documented and selected for testing to confirm their design effective and that they operated consistently throughout the period (i.e. their operating effectiveness).

We strongly recommend that clients discuss this area in detail with their external auditors to ensure that there is agreement on what will constitute an acceptable testing strategy including what should be tested and how many need to be tested. Many of the major accounting firms provide detailed guidance on the level of testing they expect to be done by management.

Related References

- PCAOB AS#2, paragraph 40 and 41

REGULATORY EXPECTATION #16: THE CEO AND CFO MUST TAKE STEPS TO ENSURE BOTH THE ADEQUACY AND RELIABILITY OF THE CONTROL ASSESSMENT AND VERIFICATION WORK THEY RELY ON TO SIGN THEIR QUARTERLY SECTION 302 AND ANNUAL 404 CONTROL EFFECTIVENESS DECLARATIONS

Expectation Guidance

In virtually all public companies the task of assessing and reporting on control effectiveness will involve a significant amount of delegation. The people involved in control effectiveness assessment and testing work may all be company employees or, alternatively, components of the work may be contracted out to firms that specialize in risk and control assessment and control verification. The company may decide to use only business unit and internal "quality assurance" staff or may involve their internal audit department in the process in various roles. Regardless of which strategy a company's selects to support SOX 302 and 404 representations, the responsibility to ensure there is adequate support for those representations rests squarely on their shoulders of the CEO and CFO.

The PCAOB in paragraph 108 states:

In all audits of internal control over financial reporting, the auditor must perform enough of the testing himself or herself so that the auditor's own work provides the principal evidence for the auditor's opinion. The auditor, may, however, use the work of others to alter the nature, timing, or extent of the work he or she otherwise would have performed. For these purposes, the work of other includes relevant work performed by internal auditors, company personnel (in addition to internal auditors), and third parties working under the direction of management or the audit committee that provides information about the effectiveness of internal control over financial reporting.

Since the PCAOB repeatedly stresses the need to assess the independence of internal staff engaged in quality assurance efforts companies should seriously consider realigning internal audit's reporting relationship if they haven't already done so, to report directly to the company's audit committee. An internal audit department that reports administratively to a CFO would not be considered to be fully independent for purposes of SOX quality assurance testing.

The PCAOB goes on to state in paragraph 109 that the auditor should:

- a. Evaluate the nature of the controls subjected to the work of others
- b. Evaluate the competence and objectivity of the individuals who performed the work
- c. Test some of the work performed by others to evaluate the quality and effectiveness of the work.

The PCAOB make it very clear in paragraph 126 that they expect that there will be some form of SOX 302/404 quality assurance process that is independent from those with primary responsibility for disclosure objectives.

As described in paragraph 40, management may test the operating effectiveness of controls using a self-assessment process. Because such an assessment is made by the same personnel who are responsible for performing the control, the individuals performing the self-assessment do not have sufficient objectivity as it relates to the subject matter. Therefore, the auditor should not use their work.

This expectation necessitates creating, maintaining or retaining some form of independent quality assurance function to ensure that the information that the CEO and CFO rely on to make their quarterly and annual representations is reliable.

CEOs and CFOs should also take steps to demonstrate that they are actively involved in the oversight of the process used to complete the assessment and the review of the results produced. These activities should be done in a way that produces evidence of the extent and frequency of their involvement.

Related References

- PCAOB AS#2 paragraphs 40-46
- PCAOB AS#2 paragraphs 108-126

REGULATORY EXPECTATION #17: MEET SEC DOCUMENT RETENTION EXPECTATIONS

Expectation Guidance

The SEC indicates on their website that they do not have specific record retention expectations for publicly traded companies. They point out that Section 13(b)(2) of the 1934 Act does, however,

require companies registered with the SEC to maintain their books, records and accounts in reasonable detail to discern transactions and dispositions of their assets.

Paisley Consulting contacted the SEC Corporate Finance Division of the Office of Chief Counsel and they confirmed on August 31, 2004 that no specific document retention rules exist as of that date related to SOX sections 302 and 404 representations.

The most direct reference we have located that indirectly relates to SOX document retention is in Footnote 76 to the SEC Section 404 Final Rule.

Section 13(b)(2)(A) of the Exchange Act [15 U.S.C.78m(b)(2)(A) requires companies to "make and keep books, records and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." See also Section 13(b)(2) (B) of the Exchange Act [15 U.S.C. 78m(b)(2)(B)] and In re Microsoft Corp., Administrative Proceedings File No. 3-10789 (June 3, 2002). In the Microsoft order, the Commission stated that such books and records include not only general ledgers and accounting entries, but also memoranda and internal corporate reports. We have previously stated, as a matter of policy, that under Section 13(b)(2) "every public company needs to establish and maintain records of sufficient accuracy to meet adequately four interrelated objectives: appropriate reflection of corporate transactions and the disposition of assets; effective administration of other facets of the issuers internal control system; preparation of the financial statements in accordance with generally accepted accounting principles; and proper auditing. "Statements of Policy Regarding the Foreign Corrupt Practices Act of 1977, Release No. 34-17500 (Jan. 29, 1981) [46 FR 11544]

Some U.S. law firms recommend that companies maintain 7 years of support documentation for SOX 302/404 representations in light of general company law and the personal and corporate implications of the Federal Sentencing Guidelines. In light of the lack of specific guidance and the complexities in this area we recommend companies consult legal counsel to determine and document rules related to document retention period for SOX 302/404 representations.

Related References

- Footnote 76 SEC Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.