
Sarbanes-Oxley Act of 2002 and Quality

Presented For:

American Society for Quality – Chicago
February 8, 2006

Presented By:

Anwer Abbasi, Chief Quality Compliance Manager
TDK Corporation of America

Brian Amend, CPA, CIA, CFSA
Protiviti, Inc.

In this Presentation

- Sarbanes-Oxley (SOX) Basics and Background
- SOX Components and Application
- Recent SOX-Related Headlines
- Linkage of SOX and Quality

Sarbanes-Oxley 101

What?

Authored by U.S. Senator Paul Sarbanes and U.S. Representative Michael Oxley, SOX represents undoubtedly the single most important piece of legislation affecting Corporate Governance, Financial Reporting and Public Accounting since the Securities Laws of the 1930's.

Why?

SOX was a direct result from large corporate financial scandals involving Enron, World Com, Global Crossing, Arthur Andersen, etc. Investor confidence in U.S. Capital Markets was shattered due to these headlines.

Who?

Essentially, SOX applies to all companies filing annual reports with the SEC under either Section 13(a) or 15(d) of the Securities Exchange Act of 1934. This applies to non-U.S. companies filing annual reports with the SEC, to small business issuers and to unlisted companies with public debt.

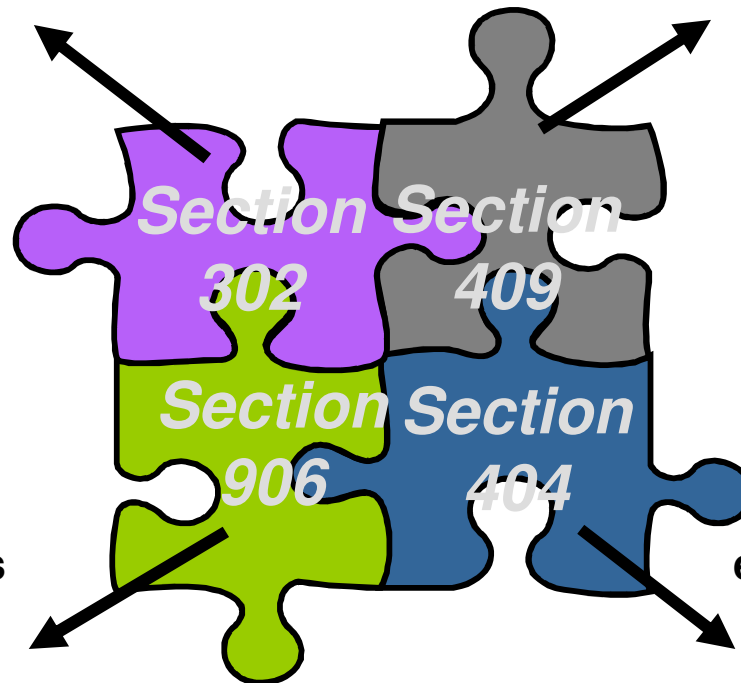
When?

Required compliance dates vary by the Act Sections, but compliance was mandatory essentially immediately upon passage of the Act.

The SOX Puzzle

Various representations by certifying officers, similar to Section 906 plus additional representations related to disclosure controls and procedures, internal controls and fraud

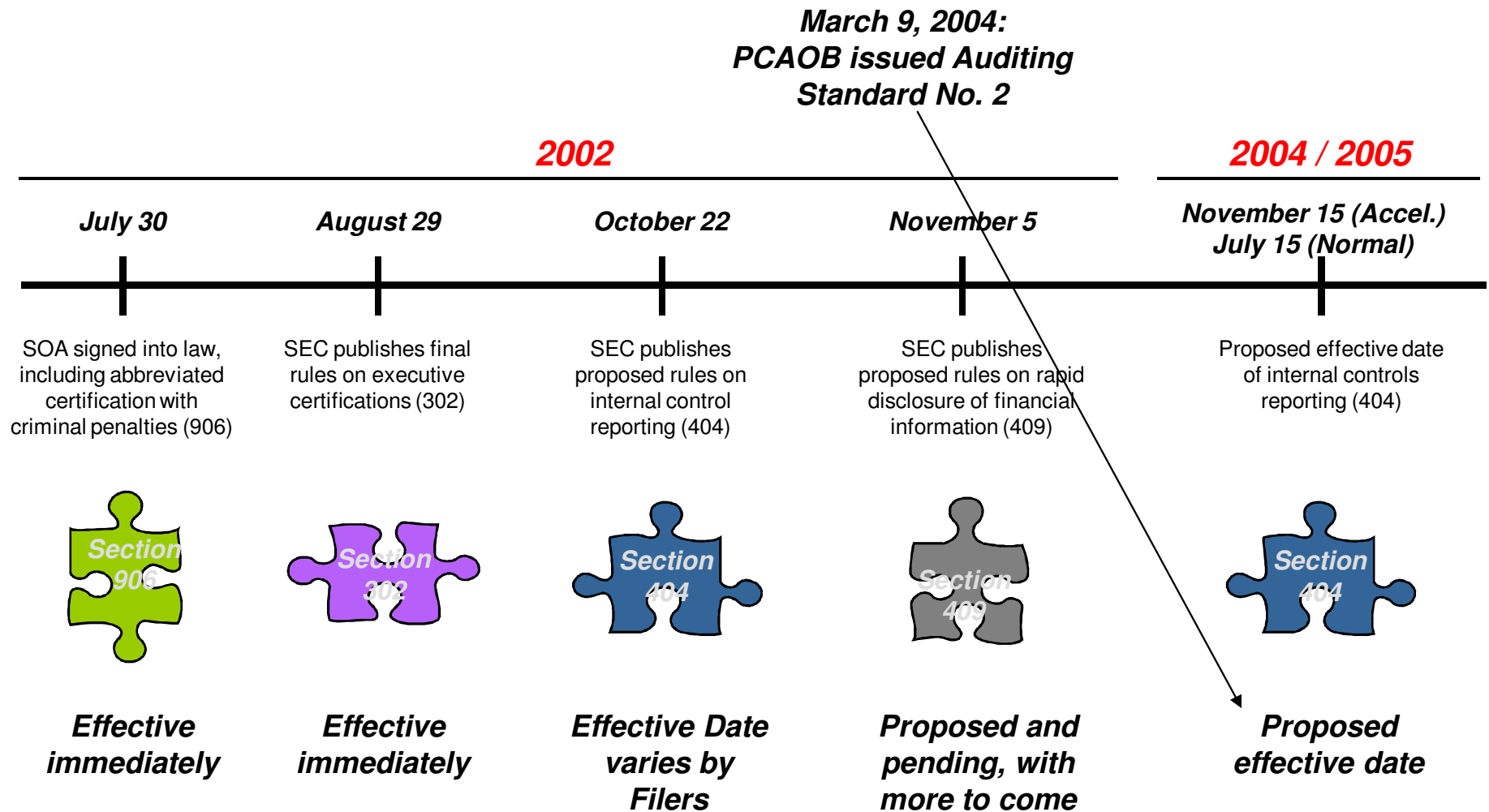
Disclose to public on a “rapid and current basis” material changes to financial condition or results of operations



The periodic report containing financial information complies with Exchange Act and fairly presents financial condition and results of operations

Perform ANNUAL assessment of the effectiveness of internal controls over financial reporting and obtain attestation from external auditors

The SOX Timeline



Sections 906 and 302 Lay the Foundation

Section 906 Certification

- Effective with Enactment of the Act, July 30, 2002
- Requires CEO and CFO to certify compliance with the SEC Exchange Act

Section 302 Certification

- Effective August 29, 2002
- Requires CEO and CFO to state much more stringent review requirements than with 906. Also, officers must assert responsibility for establishing, maintaining and evaluating disclosure controls and procedures, identify significant deficiencies and material weaknesses and fraud as well as significant changes in internal controls
- Although 302 and 906 are very similar, they differ in 3 basic aspects:
 - 1) 906 expressly imposes criminal penalties, whereas 302 relies on general criminal provision applying to all violations of the SEC Exchange Act
 - 2) 906 Certification is shorter and more narrow in scope
 - 3) Unlike 302 certifications, 906 certifications are required only in periodic reports that contain financial statements

Section 404 – Management’s Annual Internal Control Report

Management is required to file an internal control report with their annual report, stating –

- Management’s responsibilities to establish and maintain adequate internal controls and procedures for financial reporting
- Management’s conclusion on the effectiveness of these internal controls at year end
- The company’s public accountant has attested to and reported on management’s evaluation of internal controls over financial reporting

Management must evaluate design and operational effectiveness of internal controls for financial reporting (as well as its disclosure controls and procedures) on a quarterly basis

Note: On March 9, 2004, the PCAOB issued Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements. This standard is based on:

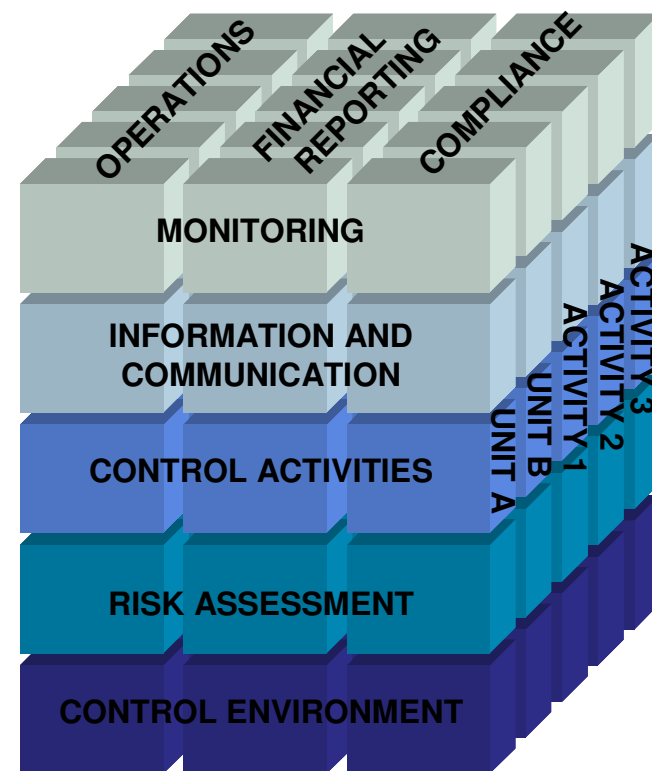
- **COSO Framework**
- **The concept of “Reasonable Assurance”**
- **A Risk-Based Approach, Focused on Financial Reporting Assertions**

The COSO Framework's Three Dimensions Provide Criteria for Evaluating Internal Controls

What is COSO?

What does it purport to achieve?

1. Requires an entity level focus and an activity level focus
2. Consists of three objectives:
 - Effectiveness and efficiency of operations (including safeguarding of assets)
 - **Reliability of financial reporting**
 - Compliance with applicable laws and regulations
3. Consists of five components:
 - Control environment
 - Risk assessment
 - Control activities
 - Information/Communication
 - Monitoring



SOX Roles – What Management Consultants Can and Cannot Do:

- Consultants can assist management in evaluating design and operating effectiveness in many ways:
 - Facilitate, enable, advise on and help document management's decisions on, design of and building of internal controls and procedures
 - By “enable”, this means to provide to management proprietary models, frameworks, processes and tools for them to use in arriving at a decision that is theirs to make
 - Consultants can also facilitate and enable the execution of client tasks as well as advise on execution
 - However, Consultants cannot conclude on the overall effectiveness of the certification or assessment process because that is fundamentally the responsibility of management

SOX Reality – Recent Reported Deficiencies

- Anchor Bancorp Wisconsin Inc. (Financial Services, \$272.3M, E&Y)
 - As reported on November 30, 2004 in the Company's amended quarterly report on Form 10-Q/A for the nine months ended September 27, 2004, because of two restatements of financial results during fiscal 2004, the Company's management concluded that a material weakness existed in its internal control over financial reporting ... The Company's management believes that the material weakness related to the Company having insufficient personnel resources and technical accounting expertise within its accounting function.
- Exide Technologies (Electronics, \$2,500.50M, PwC)
 - the Company announced that it was advised by its independent auditor, PricewaterhouseCoopers LLC, that its report on the Company's consolidated financial statements as of and for the fiscal year ended March 31, 2005 will contain a going-concern qualification ... The press release further stated that the Company's annual report on Form 10-K will report that the Company has concluded that as a result of its review of internal controls under Section 404 of the Sarbanes-Oxley Act as of fiscal year-end that there were two material weaknesses in the controls relating to the period-end financial reporting processes and the period-end accounting for income taxes.

SOX Reality – Recent Reported Deficiencies, continued

- Impax Laboratories Inc. (Pharmaceutical, \$58.89M, D&T)
 - Management has presently identified five material weaknesses in our internal controls over financial reporting as of December 31, 2004. ... The material weaknesses presently identified by management relate to: (1) the Company's Strategic Alliance Agreement with a subsidiary of Teva Pharmaceutical Industries Ltd. ("Teva") [Editor's note: issue was related to "determination of the appropriate periods in which to recognize revenues from 2004 sales of products"; (2) the Company's financial close and reporting process; (3) the Company's billing controls for non-electronic data interchange orders; (4) the Company's inventory valuation procedures; and (5) the Company's reserve for shelf stock protection.

- Delphi Corp (Automotive & Transport \$28,096M, PwC)
 - Management's assessment concluded that the Company did not maintain effective internal control over financial reporting as of December 31, 2004 as a result of the following identified material weaknesses:
 - Insufficient numbers of personnel having appropriate knowledge, experience and training in the application of GAAP at the divisional level, and insufficient personnel at the Company's headquarters to provide effective oversight and review of financial transactions;
 - Ineffective or inadequate accounting policies to ensure the proper and consistent application of GAAP throughout the organization;
 - Ineffective or inadequate controls over the administration and related accounting for contracts; and
 - Ineffective "tone" within the organization related to the discouragement, prevention or detection of management override, as well as inadequate emphasis on thorough and proper analysis of accounts and financial transactions

SOX Reality – Recent Reported Deficiencies, continued

- Polo Ralph Lauren Corp. (Consumer Products, \$3,305M, D&T)
 - Based on this evaluation, management concluded that as of April 2, 2005, the Company did not maintain effective internal control over financial reporting as there was more than a remote likelihood that a material misstatement of the Company's annual or interim financial statements with respect to income taxes would not be prevented or detected, on a timely basis, by Company employees in the normal course of performing their assigned functions.
 - This control deficiency, which management determined to be a material weakness under the Public Company Accounting Oversight Board's Auditing Standard No. 2, results from not having adequate resources with expertise in matters relating to the accounting for income taxes. Specifically, our controls related to the preparation and review of our income tax provision failed to prevent or detect errors in calculating the income tax provision and deferred income tax and income tax payable balances for the year ended April 2, 2005, which were identified by Deloitte & Touche, LLP, our independent registered public accounting firm...
 - Because of the material weakness described above, our management believes that, as of April 2, 2005, we did not maintain effective internal control over financial reporting based on the COSO criteria.

Where to find more SOX information

General Research Sites for overviews of 404 requirements and more on Protiviti's approach and tools:

Protiviti Publications

FAQ Guide to SOA 404

Guide to SOA: IT Risks and Controls

Flash Bulletins on Hot Topics and Rapid Developments

ANY Protiviti MD/Mgr/Sr

Please feel free to ask questions of ANY of our people

Other Sites for overviews of 404 requirements and implications to SEC registrants:

IIA

www.theiia.org

ISACA

www.isaca.org

AICPA

www.aicpa.org

PCAOB

www.pcaob.org

Compliance Week

www.complianceweek.com

Corporate Library

www.thecorporatelibrary.com

Shameless Plugs – Who is Protiviti?

Protiviti combines the strengths of the Big Four and Boutique alternatives ...without compromise



Protiviti Facts

- We represent more than 20% of all Fortune 1000 companies; more than 25% of all Fortune 500 companies; and more than 35% of all Fortune 100 companies.
- Client engagements vary in size: \$100K to several million
- Offices in more than 40 major markets both in the United States and internationally
- Protiviti's 2004 revenues were \$352.3 million: an increase of 164% over 2003 (\$133.3 million in annual revenues).
- Third-quarter 2005 revenues for Protiviti were \$128.2 million, an all-time high for the firm.
- For the first nine months of 2005, Protiviti generated \$350.9 million in worldwide revenues, a 54% increase over the same period in 2004. More than 2000 professionals worldwide.
- Wholly owned subsidiary of Robert Half International Inc.

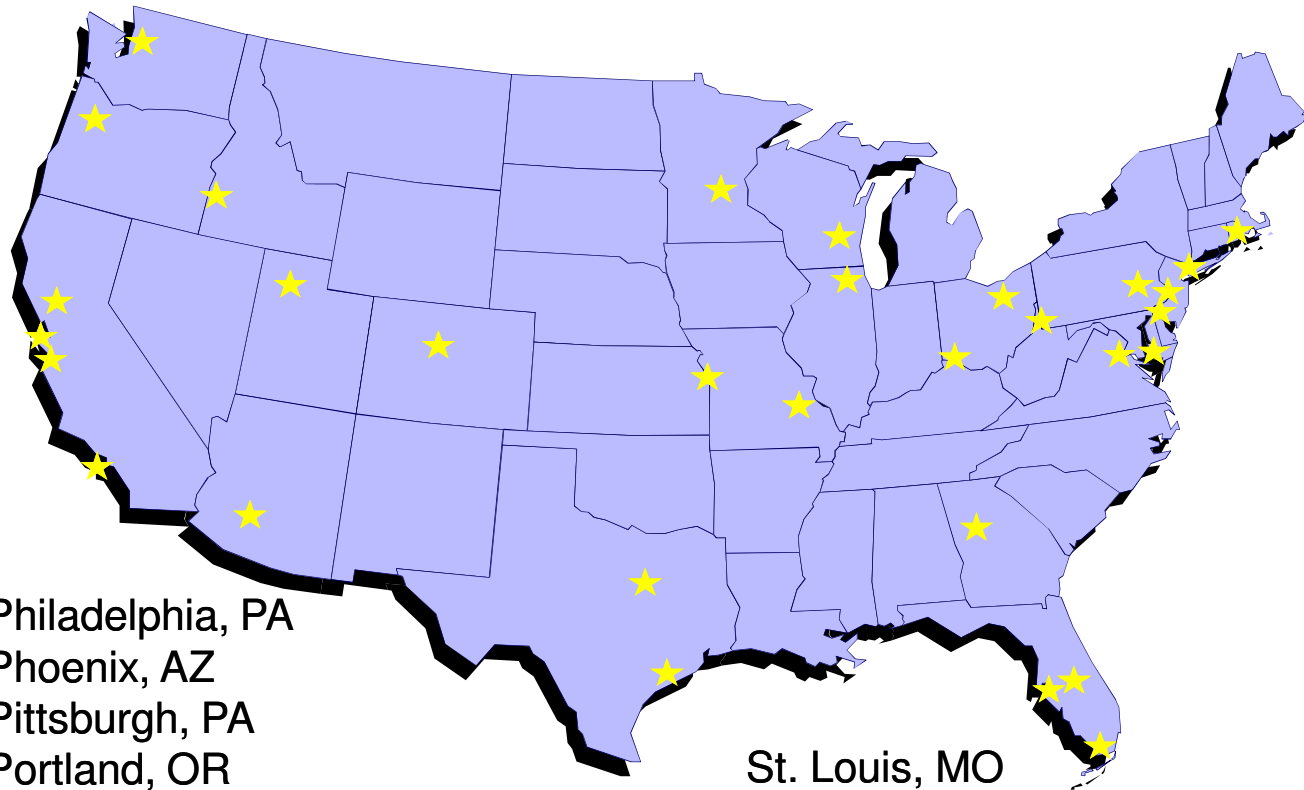
Protiviti Markets - Domestic

Atlanta, GA
Baltimore, MD
Boise, ID
Boston, MA
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Kansas City, MO
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
New York City, NY
Orlando, FL

Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Sacramento, CA
Salt Lake City, UT
San Francisco, CA

San Jose, CA
Seattle, WA
Stamford, CT

St. Louis, MO
Tampa, FL
Vienna, VA
Woodbridge, NJ



Protiviti Markets - International

- 
- **Australia**
 - Canberra
 - Melbourne
 - Sydney
 - **Canada**
 - Toronto
 - **France**
 - Paris
 - **Italy**
 - Milan
 - Rome
 - Turin
 - **Singapore**
 - Singapore
 - **Japan**
 - ◆ Tokyo
 - ◆ Osaka
 - ◆ **Korea**
 - ◆ Seoul
 - ◆ **The Netherlands**
 - ◆ Amsterdam
 - ◆ **New Zealand**
 - ◆ Auckland
 - **United Kingdom**
 - ◆ London
 - **China**
 - ◆ Beijing
 - ◆ Hong Kong
 - ◆ Shanghai
 - ◆ Shenzhen
 - **Mexico**
 - ◆ Mexico City

What we do – Internal Audit

Our Products

- Full Outsourcing
- Co-Sourcing & Specialized Resource Enhancement
- Start-up and Development Advice
- Information Technology Audit Services
- Quality Assurance Reviews
- Internal Audit Transformation
- IA Technology and Tool Implementation
- Audit Committee Advisory
- Assisting public and private companies in achieving and maintaining compliance with the Sarbanes-Oxley Act

What we do – Technology Risk

Our Products

- Security and Privacy Solutions
- Business Continuity Solutions
- Change Management Solutions
- IT Asset Management Solutions
- Program Management Solutions
- Application Effectiveness Solutions
- Technology Audit Planning and Risk Assessments
- Application Control Reviews and Internal Audits
- Security Assessments and Internal Audits
- Technology Process Controls Reviews and Internal Audits

What we do – Business Risk

Our Products

Anti-Money Laundering
Capital Projects & Construction
Corporate Security
Cost Recovery Solutions
Credit Risk Management
Energy Commodity Risk
Enterprise Risk Management
Fraud Investigation and Forensic Accounting
Litigation Consulting
Process-Based Solutions for Complying with Public
Reporting of Sarbanes-Oxley Act
Regulatory Compliance
Revenue Optimization
Supply Chain Management/Risk Consulting
Treasury Risk Management

All those in favor of a truly independent risk consulting and internal audit firm... Say **i**

protivitiSM
Independent Risk Consulting

I can no longer tell the difference between one big consulting firm and another. I am concerned about conflicts of interest. I need an unbiased specialist who can independently advise me.

I want to maximize my business and financial operations. I want to understand the implications of risk, including how to identify and manage it. I want to use the leading independent risk consulting and internal audit firm to improve my business and do it without compromise.

I do business with Protiviti. www.protiviticonsulting.com or call 1.888.556.7420

Who is TDK?



Pioneering Ferrite Core

Tokyo

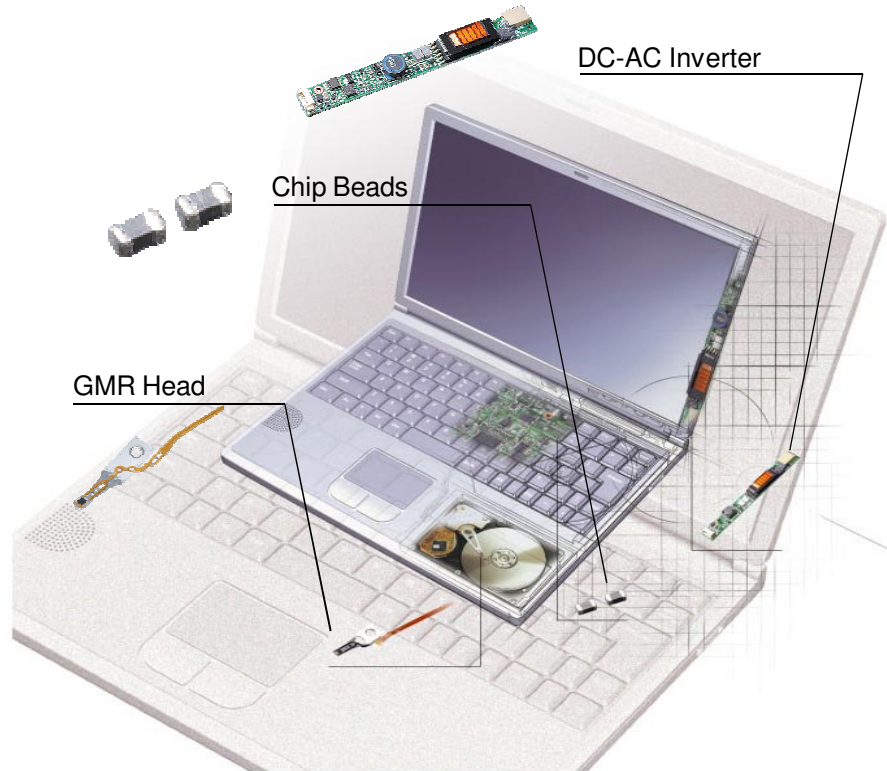
Denki (Electro)

Kagaku (Chemical)

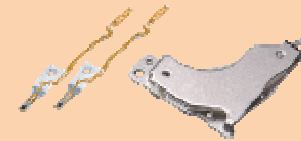
TDK Electronics Co., Ltd. was established in 1935 to commercialize ferrite, a versatile magnetic compound consisting of ferric oxide and one or more other metallic oxides. Cores, magnets, multi-layer chip components, cassette tapes and other products that incorporate ferrite still account for more than half of the company's consolidated sales.

Technologies Behind the Scenes

Always Supporting Innovations & Advances



HDD



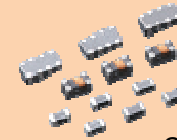
GMR Heads, VCM magnets

CPU Units, DC Power Supplies, Optical Disk Drives



Choke coils, Chip Inductors

USB/IEEE 1394 Interfaces



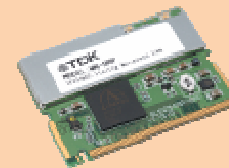
Common Mode Filters, Chip Beads

DVD Drives



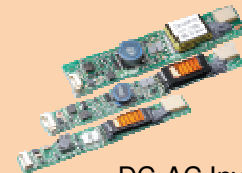
Optical Pickups, Sled Motor Magnets

Wireless LANs



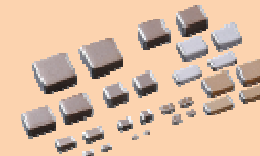
Mini PCI Modules

Liquid Crystal Displays



DC-AC Inverters

Circuit Units



Multilayer Ceramic Chip Capacitors

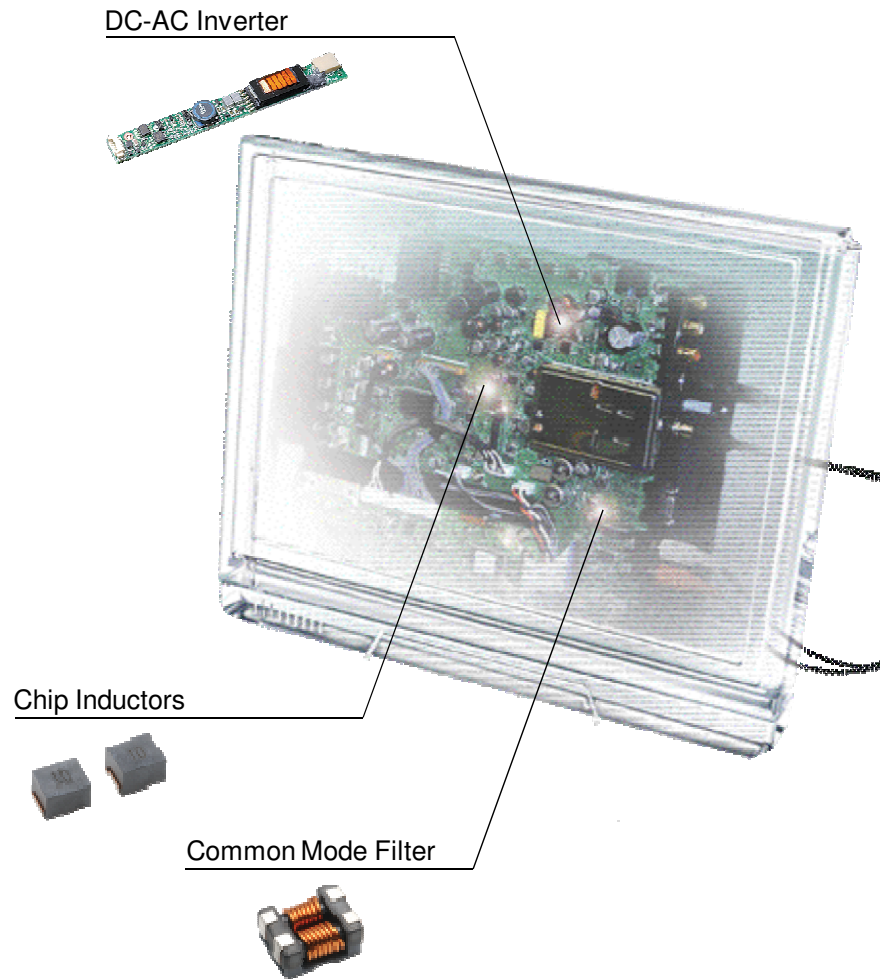
Recording Media



DVD-R, DVD-RW, DVD+R, DVD+RW

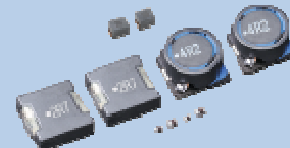
Personal Computers

Technologies Behind the Scenes



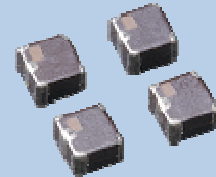
Flat Panel Display

Digital Blocks, Digital Tuners



Choke Coils, Chip Inductors

Video Signal Lines



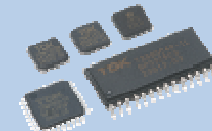
Three-Terminal Filters

Cables



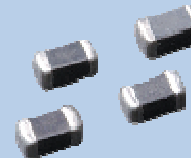
Clamp Filters

Modems, LANs, Smart Card Interfaces



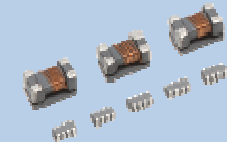
Modem ICs, LAN ICs, Smart Card Interface ICs

Flash Memory Units



Chip Beads

USB/IEEE 1394/HDMI Interfaces



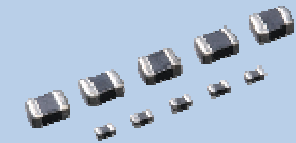
Common Mode Filters

Power Supply Circuits, Horizontal Oscillator Circuits, Circuit Units



Medium- to High-Voltage Capacitors, Multilayer Ceramic Chip Capacitors, Chip Inductors

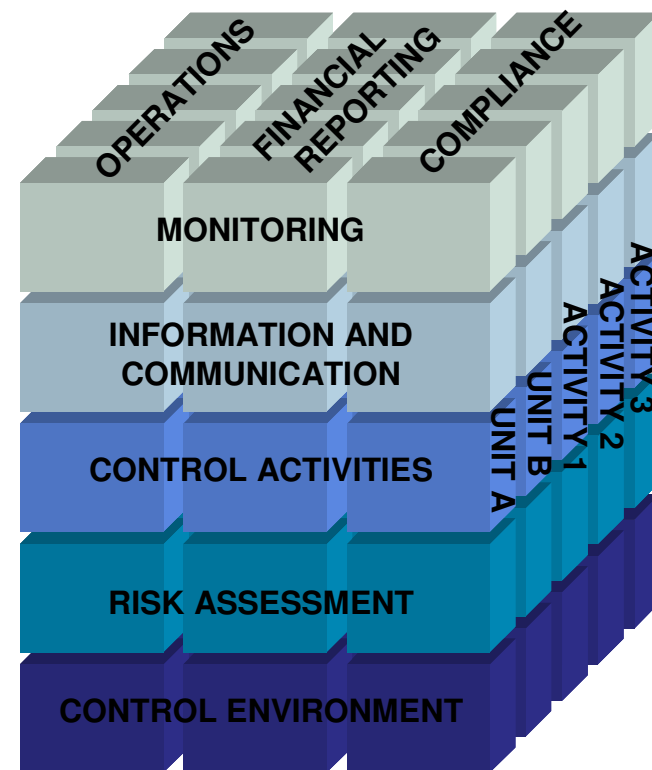
Video Input/Output Lines



Chip Varistors

COSO Framework

- 1- Monitoring
- 2- Information & Communication
- 3- Control Activities
- 4- Risk Assessment
- 5- Control Environment



Risk is the combination of the probability of an event and its consequences
(*ISO/IEC Guide 73:2002 definition 3.1.1 “Risk management – Vocabulary – Guidelines for use in standards”*)

Risk Management is the systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk

(*ISO 14971:2000, Application of Risk Management to Medical Devices definition 2.18*)

Internal Control any action, originating within the Organization, taken to manage risk. These actions may be taken to manage either the impact if the risk is realized, or the frequency of the realization of the risk

Process Owner is responsible for the process design, not for the performance of the process itself. The process owner is further responsible for the process measurement and feedback systems, the process documentation, and the training of the process performers in its structure and conduct. In essence, the process owner is the person ultimately responsible for improving a process

1- Monitoring

covers the external oversight of internal controls by management or other parties outside the process

- 5.4.1 Quality Objectives
- 5.6 Management Review
- 8.2.1 Customer Satisfaction
- 8.2.2 Internal Audit
- 8.2.3 Monitoring & Measurement of Process
- 8.2.4 Monitoring & Measurement of Product
- 8.4 Analysis of Data
- 8.5.1 Continual Improvement

How you can add-on to existing System:

No Major work needed. The Continual Improvement and Internal Audit aspect of ISO requirement provides the basis for Monitoring from Financial perspective

1- Monitoring

- Is Day-to-day monitoring being done by supervisors and process owners?
- Is Comparison done for physical assets with recorded balances, e.g., physical inventories

2- Information/Communication

supports all other control components by communicating control responsibilities to employees

- 4.2.1 General Documentation Requirements
- 4.2.2 Quality Manual
- 4.2.3 Control of Documents
- 4.2.4 Control of Records
- 5.1 Management Commitment
- 5.5.1 Responsibility & Authority
- 5.5.3 Internal Communication
- 7.2.3 Customer Communication
- 7.4.2 Purchasing Information

2- Information/Communication

- Does the process owner have access to information related to changing conditions and trends affecting the performance of the process?
- Does the process owner effectively facilitate communication within the process

3- Control Activities

are the policies, procedures, and practices that ensure the management objectives are achieved and risk mitigation strategies are carried out

- 5.6 Management Review
- 8.3 Control of Nonconforming Product
- 8.5.2 Corrective Action
- 8.5.3 Preventive Action

How you can add-on to existing System:

Expand the scope of Corrective & Preventive action procedure to include SOX deficiencies

Develop IT procedures and test them

3- Control Activities

- Are policies and procedures ensuring management directives implemented
- Are actions taken to mitigate risk
- Are the policies and procedures regularly audited

4- Risk Assessment

addresses the identification and analysis by management of relevant risks to achieving predetermined objectives

- 5.6 Management Review
- 7.2.2 Review of Requirements related to the Product
- 8.2.2 Internal Audit
- 8.2.3 Monitoring & Measurement of Process
- 8.2.4 Monitoring & Measurement of Product
- 8.4.1 Analysis of Data

How you can add-on to existing System:

Modify IQA work instructions to include elements related to SOX activities

In the Management Review include Financial objectives

4- Risk Assessment

- Has the management participated in setting of process objectives
- Does the process owner have adequate resources to achieve the objectives
- Does the process owner:
 - (a) identified significant risks in the Process
 - (b) assess the likelihood of occurrence of risk; and
 - (c) evaluated actions for reducing risks?

5- Internal Control Environment

puts responsibility on management to assign authority & responsibility, organize and develop its people as well as provide effective mode of Communication

- 5.1 Management Commitment
- 5.3 The quality policy
- 5.4.1 Measurable Objectives
- 5.5.3 Internal Communication
- 5.5.1 Responsibility & Authority
- 6.1 Provision of Resources
- 7.1 Planning Product Realization & Measurement

How you can add-on to existing System:

Include financial policies, procedures & records as part of communication along with other items being addressed in the company.

Make financial indices part of Management Review

5- Internal Control Environment

- Has the process owner documented and communicated policies/procedures
- Is there a Control over access to sensitive and critical applications and data
- Do process personnel understand their roles and responsibilities

SOX vs. ISO

SOX

Process Outline

Flowcharts

Risk Control Matrix

Test Plan

Gap logs

ISO

Manual

Procedures

Control Plan

IQA Schedule

IQA findings

Documenting Risk Assessment

Description of Work	Risk	Magnitude of Risk		Controls in Place	Action Planned	Target Date	Owner	Related W/I
		Impact	Likelihood					
To ship the Product On-Time	Raw Materials not received on time from Supplier A	High	Low	Contact Alternate Supplier	Put Supplier A on Black List	Sept	Material Manager	ABC-001
	Worker A, B called in Sick	High	Low	Contact Temp Agency			Plant Manager	CDE-002
Print Invoice for Shipment	Printer not Working	High	Low	Use Stand-by Printer	Contact IT dept		Warehouse Manager	ZXC-004

What Quality professionals can do ?

- Study SOX and COSO requirements
- Understand the Tone of Company
- Document the Procedures for Financial activities
- Document how to Test (Audit) the Procedures, Processes and Data
- Conduct Risk Assessment based on documented procedures
- Assign Action Items to the Related Process Owners
- Follow-up on ACTION Items and
- Have these Action Items closed with the supporting documented evidence

Questions to SOX Expert

Question 1:

The SEC estimates that it will cost \$91,000 annually in order to be in compliance with just Sec. 404. Is it really worth it?

Answer:

Try looking at it from another angle:

Cost of compliance: \$91,000.

Not being a convicted felon: **Priceless**

Question 2:

The janitor told me that shredders are now illegal. Is this true?

Answer:

Is your janitor a former Arthur Andersen Partner?

Shredding is now a tricky process and proper data retention is imperative

Source: SOX-Online.com

Thank you

Bibliography

- *Two Controls, One Result: Quality Progress July 05- Andy Hoffman*
- *The Orange Book: Management of Risks-Principles & Concepts Oct 2004: HM Treasury*
- *Sox-Online.com*
- *Flowhelp.com*