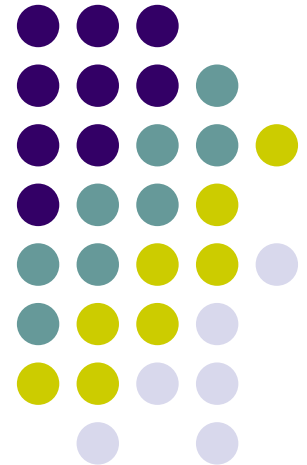


Thompson, Cobb, Bazilio & Associates, PC (TCBA)

eRisk and Liability in On-Line Transactions – the impact of Sarbanes-Oxley (SOX)

May 26, 2006

**Presented by: Ralph Bazilio,
President, TCBA**





AGENDA

- ❖ Personal Background
- ❖ What is eRisk and Liability
- ❖ Overview of SOX
- ❖ Impact of SOX
- ❖ Steps to take to manage eRisk and Liability



What is eRisk and Liability?

- ❖ eRisk is the RISK associated with engaging in ebusiness or ecommerce.
- ❖ NIST defines RISK as the negative impact of the exploitation of a vulnerability, considering both the probability and the impact of occurrence.
- ❖ The consequence or impact of a fully exploited vulnerability often leads to a LIABILITY – someone or an entity will be held responsible.

Some of the risks of engaging in On-Line Transactions (ecommerce)



- Hackers and Viruses
- Privacy Issue – Laws and Regulations
- Control of third party service providers
- Poor or obsolete technology
- Employee errors and mistakes
- Inadequate back office support
- Lack of adequate policies and procedures

Overview of SOX



- ❖ A major crisis in corporate governance in the US led to the passage of Sarbanes-Oxley Act in July 2002.
- ❖ The public became very suspicious of financial reporting.
- ❖ The purpose was to restore confidence in the reliability of Companies' financial reporting.
- ❖ Section 404 of SOX came about as a direct result of corporate failures
- ❖ CEOs and CFOs must now certify financial statements.

Overview of SOX (continued)



- ❖ Management of publicly traded companies must now report annually on the effectiveness of the Company's internal controls.
- ❖ External auditors have to attest to management's evaluation of the effectiveness of the controls.
- ❖ Requires companies to use a suitable internal control framework. The SEC recommends, but does not require COSO as a "suitable" framework

The Impact of SOX



- Business executives are held personally accountable – just yesterday two executives of Enron were found guilty.
- Full employment for us (CPAs and IT consulting firms).
- The financial reporting process and systems must be assessed for compliance with SOX.
- Very little guidance exist on selecting and implementing a suitable internal control framework

Steps to Take to Manage eRisk



- ❖ Some questions to ask:
 - Do you have internal resources to address this?
 - Have you had a Risk Assessment done?
 - What laws and regulations impact your business?
- ❖ The best approach is a comprehensive Risk Management Plan
- ❖ Develop, implement and maintain the plan
- ❖ Obtain outside assistance if you need it.

Questions and Answers

