Sarbanes-Oxley and Business Continuity

Bob Janusaitis, CISA, CISM, CBCP
Business911 International, Inc.

ACP Houston Chapter
January 13, 2004

About us

Business911 International, Inc. established in 1996, provides comprehensive enterprise-wide, expert guidance on IT Governance and Information Technology Risk Management.

•- Independent IT Audit outsourcing or gap analysis utilizing COBIT
•- Sarbanes-Oxley Section 404 IT compliance reviews
•- SAS 70 reviews
•- Security Assessments
•- Disaster Recovery and Business Continuity Planning
•- Emergency Response and Crisis Management

Business Continuity planning software includes:
•- Integriti™ and Integriti.Online™

Legal Disclaimer

The presenter today has used his best efforts in preparation of this material to increase your awareness of Sarbanes-Oxley issues. Any suggestions make no warranty, expressed or implied and are not a substitute for legal advice.


12:00

Discussion outline

- What is it and why was it enacted?
- Who does it affect?
- Where does Business Continuity fit?
- What should we do now?
- Q&A

What is it?

Legislation enacted post Enron/Worldcom events

What is the purpose of SOX

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

Who does it affect?

AMERICAN STOCK EXCHANGE

NASDAQ

Timeline

- Sarbanes-Oxley enacted January 2002
- All companies were going to have to fully comply by December 2003, but
- The SEC didn’t issue it’s final rulings on Section 404 until October 2003
- Extended Section 404 compliance until December 2004 (in most cases)

Section 404

Section 404, requiring the Commission to adopt rules requiring a company's management to present an internal control report in the company's annual report containing: (1) a statement of the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) an assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting. Section 404 also requires the company's registered public accounting firm to attest to, and report on, management's assessment.

What were they waiting for?

- They had to establish new standards or use standards already in existence
- SEC finally decided on COSO which applies to Financial Reporting

Committee Of Sponsoring Organizations (COSO)

COSO is a voluntary, private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector organization often referred to as the Treadway Commission. The sponsoring organizations include the AICPA, American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA).

But does not include Information Systems Audit and Control Association (ISACA) for whatever reason

COSO Components

Illustrating COSO at the Entity Level

COSO Component	Attributes
Risk Assessment	▪ Entity-wide objectives ▪ Activity-level objectives ▪ Risk identification and assessment ▪ Managing change
Control Environment	▪ Integrity and ethical values ▪ Commitment to competence ▪ Board of directors or audit committee ▪ Management's philosophy and operating style ▪ Organizational structure ▪ Assignment of authority and responsibility ▪ Human resource policies and practices
Information and Communication	▪ External and internal information is identified, captured, processed and reported ▪ Effective communication down, across, up the organization
Control Activities	▪ Policies, procedures and actions to address risks to achievement of stated objectives
Monitoring	▪ Ongoing monitoring ▪ Separate evaluations ▪ Reporting deficiencies

Points of Focus

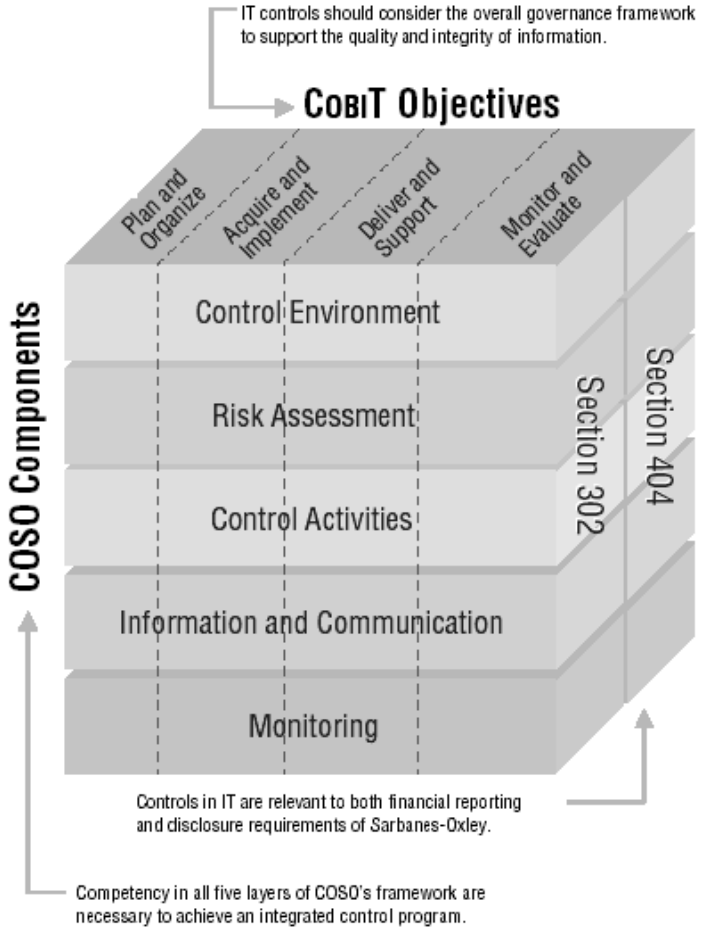
- Are there policies, procedures and effective processes for hiring, compensating, promoting, training and terminating employees?
- Are employees made aware of their roles, responsibilities, authorities and performance expectations?
- Are everyone's control-related responsibilities clearly articulated?
- Are employees accountable for results and are performance expectations reinforced with appropriate performance measures?
- Are employee retention and promotion criteria clearly defined, and is the performance evaluation process effective?
- Does management take appropriate remedial action in response to departures from approved policies and procedures?
- Is the established code of conduct reinforced and disciplinary action taken when warranted?
- Are the background and experience of prospective employees checked and references obtained?

Source: COSO Internal Controls – Integrated Framework, Framework and Evaluation Tools

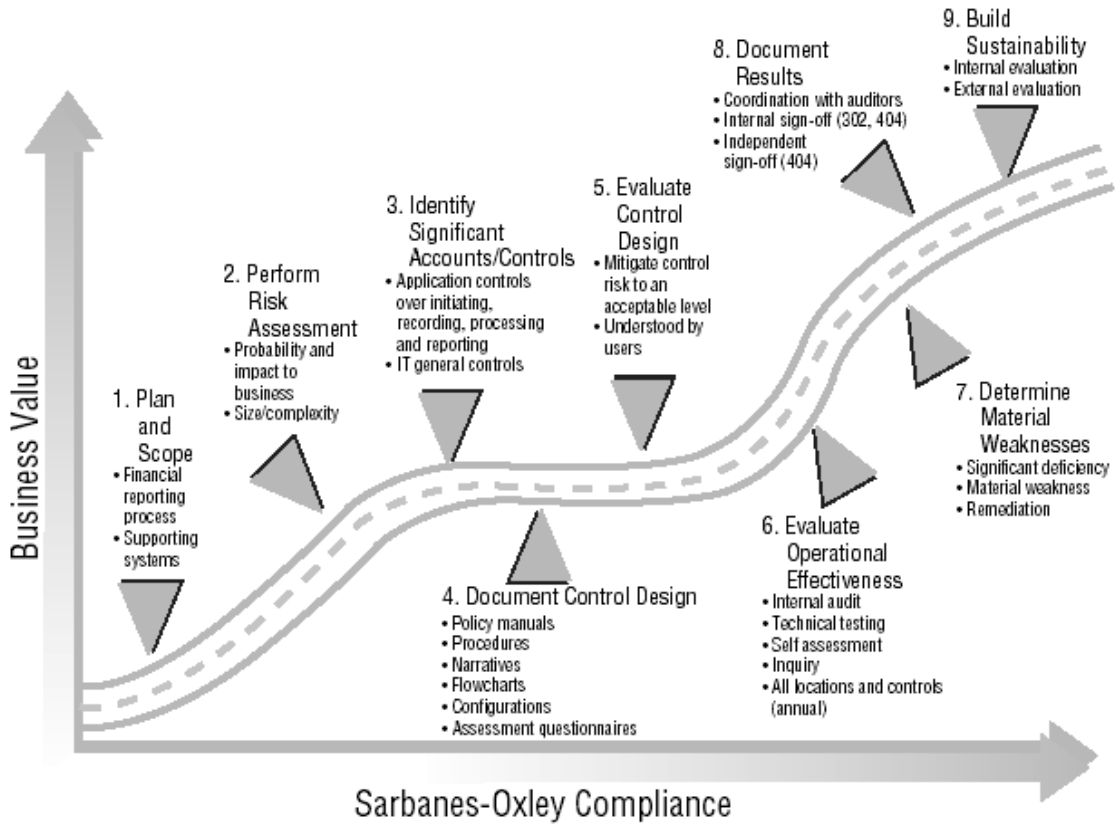
Problem?

- It did not address the IT aspect of the records
- Control Objectives for Information Technology (COBIT) existed as an international standard, but it was a stand alone standard
- IT Governance Institute commissioned a study to map COSO to COBIT

COBIT components



IT Governance perspective



Stages of Control Reliability –where are you?

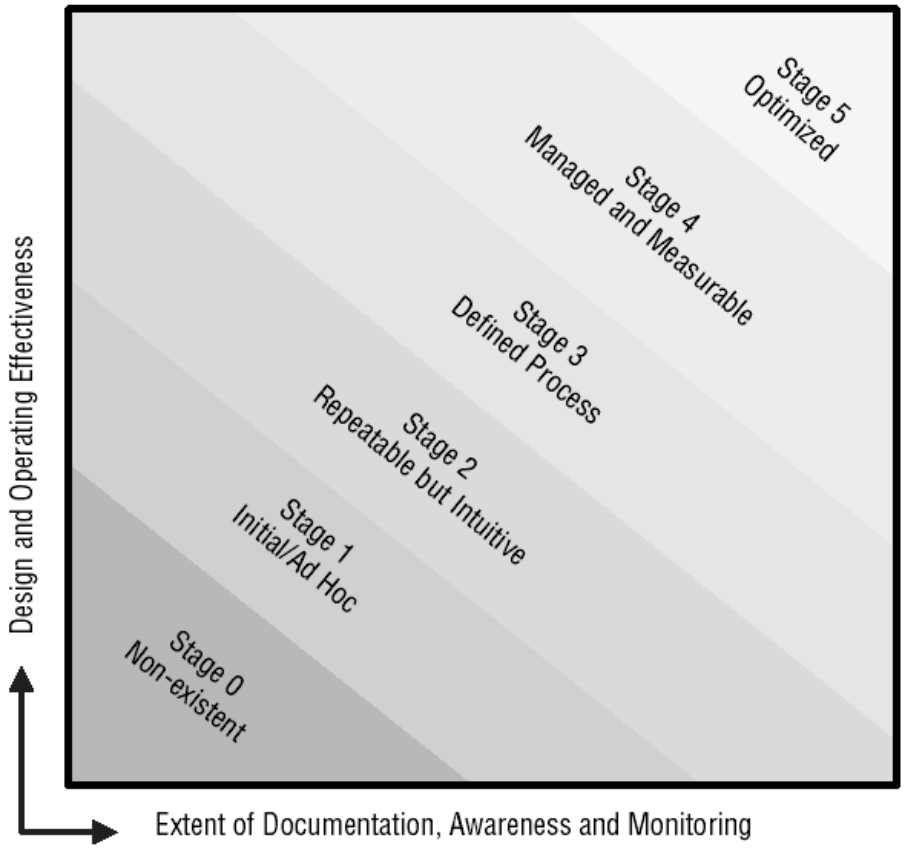


Figure 23—Manage Third-party Service Levels

Control Objective	COSO Component
Managing third-party services includes the use of outsourced service providers to support financial applications and related systems. Actions performed in this area align with the control environment, monitoring, control activities and risk assessment components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, insufficient controls over processing accuracy by a third-party service provider may result in inaccurate financial results.	
IT management ensures that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and their financial viability.	Control environment
Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Control activities
Business continuity controls consider business risk related to third-party service providers in terms of continuity of service, and escrow contracts exist where appropriate.	Risk assessment
Procedures exist and are followed to ensure that a formal contract is defined and agreed to for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	Control activities
A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	Control activities
A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	Monitoring

Figure 25—Ensure Continuous Service

Control Objective	COSO Component
Managing continuous service includes the ability to recover from a disaster. Controls need to be in place to manage various disaster scenarios, from backup and recovery to full business continuity. Actions performed in this area align with the control activities and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, the inability to recover from a disaster after year-end could prevent the organization from producing financial reports that are supported with source documentation and details of transactions that make up financial reporting balances.	
IT management, in cooperation with business process owners, has established a business continuity framework that defines the roles, responsibilities, risk-based approach/methodology to be adopted, and the approval procedures.	Control activities
The business continuity plan identifies the critical application programs, third-party services, operating systems, personnel and supplies, data files, and time frames needed for recovery.	Control activities
The IT continuity plan is aligned with the overall business continuity plan to ensure consistency.	Control activities
The IT organization's members responsible for disaster continuity plans have been trained regarding the procedures to be followed in case of an incident or disaster.	Control activities

IT management has ensured that the continuity plan is adequately tested, at least annually, and that any deficiencies are addressed within a reasonable period of time.	Control activities
Where new risks are identified, appropriate changes are made to the business continuity and disaster recovery plans.	Control activities
Offsite storage and recovery facilities are periodically assessed, at least annually, for viability, adequacy and security mechanisms.	Monitoring
A business impact assessment has been performed that considers the impact of systems failure on the financial reporting and disclosure process.	Control activities
Management has reviewed the impact assessment in determining the nature and extent of system recovery procedures necessary to support the timeliness of financial reporting and disclosure processes.	Control activities

Top 5 indicators you have a problem

- You don’t have a tested plan
- You’re IT group doesn’t think SOX affects them
- You still have to explain the concept of Business Continuity
- You have a culture of documentation phobia
- Management thinks Sarbanes-Oxley is a legal firm

What should we do now?

- Make sure management understands without a BCP plan they will most likely not get sign off by the external auditors
- This is not Y2K, it is an ongoing requirement that requires financial commitment and personnel
- Meet with your internal auditors and determine what specifics they may require

Acknowledgments

- Information Systems Audit and Control Association
- IT Governance Institute