What Does Sarbanes-Oxley Have to Do with the Management of Databases?

nocoug May 2006

Steve Lemme
Director Product Management
CA
Steve.lemme@ca.com

Abstract

- Foremost in the minds in business executives today is how to meet new regulatory compliance and corporate governance. New laws are changing the way companies collect, retain, and manage information. DBAs need to understand what is happening in the corporate business world and how it will directly impact their role.

Disclaimer

- Information presented in this presentation represents a personnel perspective from a DBA on Sarbanes-Oxley topic matter in relation to database management
- Presenter makes no representation, warranties or assurances from this presentation perspective
- Presenter makes no claim use of information in presentation will assure any outcome
- This presentation has not been validated by any auditors
- Refer to last slide for additional sources of information
- Where advisement is sought, seek help from accounting or legal professionals

Key Regulations

Legislation	Purpose
HIPAA, FDA 21 CFR Part 11	Addresses security and privacy of health data
Gramm-Leach-Biley Act	Protect consumers' personal financial information held by financial institutions
Patriot Act	To deter terrorist acts and enhance law enforcement investigation
Calif. Senate Bill 1386	Disclose any compromise of customer data to every affected consumer residing in California within 48 hours
VISA CISP	Protect, restrict and track data access to customer credit card information
Canada	Protecting personal information that is collected, used or disclosed
Sarbanes-Oxley Act Financials assurance	Information assurance for sensitive corporate data (confidentiality, audit)

No Public Company Spared

Industry Samples	Sarbanes-Oxley	HIPAA	Gramm-Leach-Biley	Patriot Act	California Senate Bill 1386	VISA CSSIP Mastercard SDP AMEX
Financial Institutions	✓		✓	✓		
Healthcare Industry	✓	✓				
Credit card Processing	✓					✓
Insurance	✓	✓				
Manufacturing	✓					
Telco	✓			✓		
Retail	✓					✓
Academia	✓		✓	✓ SEVIS		
Collect bank or SSN	✓		✓	✓		
Company storing CA resident info	✓				✓	

Compliance and Governance Overview

- Sarbanes-Oxley Act (SOX)
  - Signed into law by US Congress in 7/2002
  - Reaction to financial fall of several publicly traded companies
  - Applicable to all public companies
- Several Act sections stand out
  - Section 103
    - Audit companies assurances that clients implement internal control and procedures that ensure accurate recording and maintenance of financial information
  - Section 302
    - CFOs and CEOs certify quarterly they are responsible for disclosure of design and operational effectiveness of controls
  - Section 404
    - Annual reporting contains internal control assessment report to provide assurance that financial statements are accurate
    - Not only assure controls are in place, provide auditors with demonstration and documentation supporting assessment

SOX 404

- Company Management
  - Assures evaluation of controls effectiveness
  - Provides written assessment
  - Accepts responsibility for it
  - Supports audit evaluation with evidence
- Definition of control/control activity
  - Safeguards or processes that mitigate risk
  - Processes effected by people designed to accomplish specified objectives (COSO)
  - Infrastructure, and other components maintain confidentiality, integrity, availability

Compliance With Sarbanes-Oxley

- Section 404 requires external auditor's opinion on effectiveness of internal controls
- Ability to demonstrate controls implemented for quarterly certification
- Standards and repeatability play a critical role in demonstrating adequacy of controls for data integrity
- If controls can be bypassed, management cannot with certainty attest to integrity, confidentiality and non-repudiation of financial reporting
- Initial round of review many tried best to document with the help of an auditing firm

So Far What Has Been Learned

- 53% of control deficiencies were within routine processes
  - Leading areas for significant remediation included IT (72%)
- One-fourth of companies with over $20 billion in revenues tested more than 10,000 controls
  - 42% of companies required 2 to 4 hours to test each control on average
- Factors likely to increases the prospects of a material weakness for companies
  - Heavy dependence on automation without sufficient in-house information technology personnel
- Of the 77% of companies that have or intend to institute a formal, company-wide approach to risk assessment, only 25% have a mature approach currently in place
  - According to an Ernst & Young Emerging Trends in Internal Controls survey September 2005 http://www.sarbanes-oxley.be/aabs_emerging_trends_survey4.pdf

IT Implications

- Controls related to initiating, authorizing, recording, processing, and reporting of financial data
  - General Controls
    - Security (logical and physical)
    - Change management
    - Back-up and recovery
    - Job scheduling and operations, etc.
  - Application Controls
    - Input, output, alteration and validation of data
    - Disallowance of duplicate transactions
    - Processing error correction
    - Processing report accuracy

From The Outside

- General Control
  - Across all systems provide control foundation for applications, implementations, maintenance, security access, segregation of duties, etc…
    - For example - logging of unsuccessful attempts to access UNIX operating system eBusiness Suite resides on
- Application Control
  - Ensure processes related to transactions are complete and correct
    - For example – An order is taken over the Internet and the sale is authorized upon entry of a valid credit card number

From The Inside

- Infrastructure control
  - Causing obstruction or delay of data availability
- Database structure control
  - Object change affecting financial reporting
    - Like deleting a column in a table that contains financial results for Q4
- Database data control
  - Changes to values within a database table
    - Like inventory or sales data

Inventory And Identify

- All financial system databases or databases they exchange data with
- All access methods with capabilities to alter their data
- All risks that could expose the data to alteration; accidental or deliberate
- The people, processes, and technology involved

Control Review

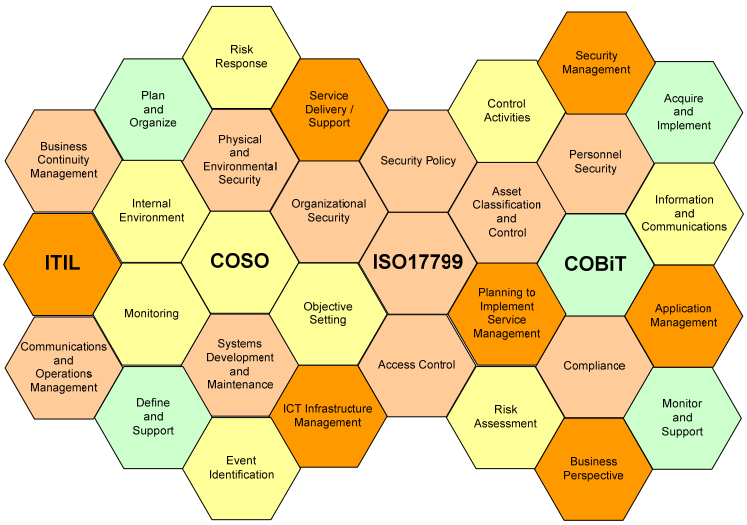
- Re-evaluate quarterly or when a change occurs that could impact reporting
  - Mergers and acquisitions
  - New system implementations and alterations
  - Business needs change
  - Technologies change
  - When disaster strikes
    - Physical like an earthquake
    - External threat like a major virus

Question

How many have implemented controls to meet Sarbanes-Oxley compliance?

1. Implemented manual controls and do not plan to automate
2. Implemented manual controls and plan to automate
3. Majority of controls are automated

Compliance Is About Methods and Controls



Repeatable Best Practices

What Control Framework does your company utilize?

- COSO
- Full COBiT
- SOX only subset of COBiT
- ITIL
- Homegrown
- Have no Control Framework

COSO Internal Control Framework

- Committee of the Sponsoring Organizations, Treadway Commission (COSO) provides a general framework for internal controls
  - Control environment - tone of organization, influencing control consciousness of its people
    - Integrity, ethical values and competence
  - Risk assessment – assess risks from external and internal sources
    - Identify, analyze, and manage risks pertaining to business objectives
  - Control activities
    - Control policies and procedures to address identified risks to ensure directives are accomplished
  - Information and communication
    - Enable people to capture and exchange information needed to contact, manage, and control operations
    - Pertinent information identified, captured, exchanged in a form and timeframe enabling staff to perform responsibilities
  - Monitoring
    - Ensure processes assessed regularly and modified to ensure control
- An accounting standard, not Information Technology

SOX, COSO and COBiT

- SOX regulation commentary to standards for internal controls sections 302, 404
  - Often applied to derive specific IT control requirements in a SOX-regulated environment
- Control Objectives for Information and related Technology (COBiT)
  - Created by Information Technology Governance Institute (ITGI)
  - Framework of control objectives focusing on IT governance specific to the IT environment
  - COBiT provides a framework that helps define IT's role and control responsibilities

Accountability Includes Databases

- A DBA said she was assigned a project for "SARBOX"
  - Just needed to verify access on a number of tables
  - But in actuality, it is much more
- **Computer Operations - COBiT**
  - Includes controls over definition, acquisition, installation, configuration, integration and maintenance of IT infrastructure
  - Includes controls over acquisition, implementation, configuration and maintenance of operating system software, database management systems, middleware software, communications software, security software and utilities that run the system and enable financial applications to function

COBiT

- CobiT framework consists of four domains comprising at least 34 IT processes and 225 control objectives
  - Aligns with the general COSO framework for internal controls
  - IT control processes that address governance of the enterprise data environment including
    - Acquire and Maintain Application Software
    - Acquire and Maintain Technology Infrastructure
    - Ensure Systems Security
    - Manage the Configuration
    - Manage Problems and Incidents
    - Manage Data
    - Manage Operations

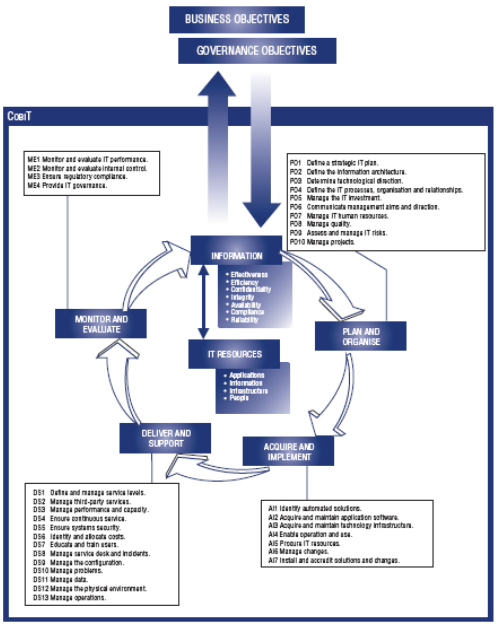


Figure 16 – Overall COBiT Framework
COBiT 4.0 whitepaper ISBN 1-933284-37-4 - Shown for academic use only

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

Processes And Controls

- Prevent
  - Authorized users accessing or altering data accidentally or deliberately
  - Unauthorized access or changes resulting in incorrect financial reporting
  - Gaps in policy or procedures making data vulnerable to access or change
- Key Controls include
  - Separation of duties
  - Effective change management
  - Effective change documentation
  - Release processes
  - Control processes
  - Resolution processes

Controls for Databases

- Identify relevant database controls
- Identify risk for each control objective
- Identify relevant control activities
- Documentation
- Communication
- Monitoring
- Evaluation of design effectiveness
- Testing of operations effectiveness

Effectiveness Maturity

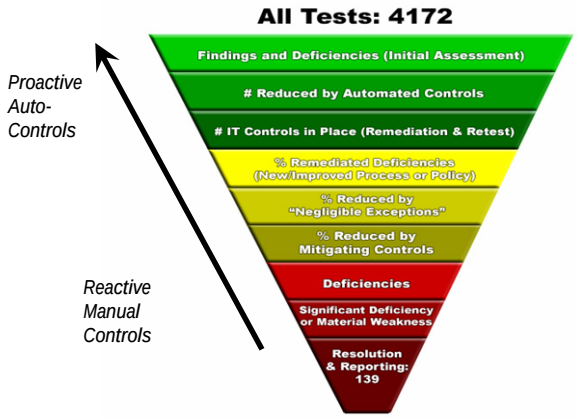
- **Unreliable**
  - Policies and procedures not documented
  - Staff not aware of control responsibilities
  - No measurement or monitoring
- **Insufficient**
  - Controls exist but not documented or demonstrated
  - Monitoring, violations reported but process not documented
  - Some aware of control responsibilities
  - Effectiveness of controls not evaluated on a regular basis or take to long to fix
- **Effective**
  - Controls documented, can be demonstrated
  - Staff aware of their control responsibilities
  - Monitoring, reporting, escalating and reporting effective, documented
  - Deficiencies identified and remedied in a timely manner
- **Established and Repeatable**
  - Annual enterprise-wide risk management
  - Staff continuously made aware of responsibilities
  - Real-time monitoring, periodic self-assessment
  - Gaps remedied as they are discovered
  - Minimal effort on documentation updates, testing, and remediation

Control Audit Example

- Evaluating controls documented by DBAs, automated reports run daily, but no review
  - Reports should be reviewed, researched for exceptions, and then reported routinely to IT Manager
- DBAs run automated reports, summarize exceptions, but no escalation
  - Reporting of exceptions only occurred monthly
  - Worked performed by DBAs is insufficient

SOX Automation

Reduce deficiencies through automation and integration



Deficiency Categories:

- Segregation of Duties & Access
- Audit Trails & Approvals
- Change Management
- Back Up / Retention of Info.

To Start

- Database Change Management
  - Managing object permissions, or schema changes to eliminate risk of unauthorized viewing, altering, or copying of data
  - Audit validation of changes as authorized or unauthorized
  - Rapid analysis and response when unauthorized changes occur
- Database Log Auditing
  - Ensure protection of database transaction logs from alteration and deletion
  - Routinely review database logs to verify approved modifications and identify unauthorized changes
- Database Backup & Recovery
  - Demonstrating recoverability within reasonable business continuance
  - Database archival, backups, loading and unloading, routinely verified to ensure that data is secured

Review and Preparation

- Data integrity ownership and responsibilities communicated to appropriate data/business owners acceptance of responsibilities
- Key database systems inventoried and owners identified
- Database Management staff understands and accepts their responsibility regarding internal controls
- Division of roles and responsibilities (segregation of duties) that prevents a single DBA from unauthorized alterations
- Review documented Database Management processes
- Review documented Database Management risks
- Documented Database Management process controls
- Testing of Database Management control methods
- Gap identification and controls improvement process
- Update Database Management processes and document controls

Ongoing Quarterly Review

- Sarbox does not mandate software, however technology and automation ease the compliance process
  - As compared to manual or paper-based processes
  - Auditors seek consistent and repeatable processes and controls
  - Software solutions enable great consistency and help automate controls

Standards and Process

- Auditors may use standards such as COBiT for IT controls and objectives
  - COBiT approaches IT controls looking at information and data that supports business requirements and associated IT resources and processes
  - Don't create a non-standard approach, when you can leverage something known by an auditor

Industry Organizations

- Industry Organizations
  - www.isaca.org
  - www.coso.org
  - http://www.aicpa.org/news/2004/2004_0929.htm
  - www.auditnet.org/sox.htm
  - http://www.itgi.org/

Further Information, Questions?

Technology is Available to Help

- One of the world's largest management software companies, delivering software and services across operations, security, storage, life cycle and service management to optimize the performance, reliability and efficiency of enterprise IT environments.

CA database compliance whitepaper
http://www3.ca.com/Files/WhitePapers/reg_compliance_db_manage_wp_en_us.pdf

CA Technology to assist with compliance
www.ca.com/compliance

- CA technology for multi-database management
  - www.ca.com/databasemanagement

- And you can also use the new Database Command Center
  - Assists with control and automation
  - At "No Charge"
  - www.ca.com/unicenterdcc