



The
University
of Akron
—
College of
Business
Administration



Symposium on Information Systems Risk, Security & Assurance
February 25, 2005

Sarbanes-Oxley and the Assessment of Integrity of Financial Information Systems

David Handal
Director, Risk Advisory Services

Jai Cullath
Senior Associate, Risk Advisory Services

Information Risk Management
February 25, 2005

AUDIT ■ TAX ■ ADVISORY



Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
7. Evaluation of Control Deficiencies
8. IT Controls –Top Deficiencies

Contents / Agenda

- 1. Overview of Sarbanes-Oxley (SOX) Section 404**
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
7. Evaluation of Control Deficiencies
8. IT Controls –Top Deficiencies

Sarbanes-Oxley (SOX) Section 404

- ◆ **Section 404 of the Sarbanes-Oxley Act of 2002 requires:**
 - Company management to assess and report on the company's Internal Control Over Financial Reporting (ICOFR).
 - The company's external auditors to issue an "attestation" to management's assessment.
- ◆ **The company's external auditor must report directly on the effectiveness of ICOFR.**

Sarbanes-Oxley (SOX) Section 404

- ◆ Accelerated filers are generally U.S. companies that have equity market capitalization over \$75 million (and have filed at least one annual report with the SEC).
- ◆ Accelerated filers are required to comply for fiscal years ending on or after November 15, 2004, others have until fiscal years ending on or after July 15, 2005 to comply.
- ◆ Accelerated filers with less than \$700 million in “public float” have an extra 45 days to file both the management and auditors’ report on ICOFR.

What is Internal Control Over Financial Reporting (ICOFR)

A process *designed by, or under the supervision of*, the company's *principal executive and principal financial officers*, or persons performing similar functions, and

- *effected by the company's board of directors, management, and other personnel,*
- **to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes**
- *in accordance with generally accepted accounting principles*

Objective of Internal Control Over Financial Reporting (ICOFR)

The objective of an audit of ICOFR is to express an opinion on management's assessment of the effectiveness of the company's internal control over financial reporting

- To form a basis for expressing such an opinion, the auditor must plan and perform the audit to obtain reasonable assurance that no material weaknesses exist as of the date specified in management's assessment.

Management's Responsibilities in ICOFR

- ◆ **Accept** responsibility for the effectiveness of the company's ICOFR.
- ◆ **Evaluate** the effectiveness of the company's ICOFR using suitable control criteria.
- ◆ **Support** its evaluation with sufficient evidence, including documentation.
- ◆ **Present** a written assertion about the effectiveness of the company's ICOFR.

Auditor's Responsibilities in ICOFR

- ◆ Must obtain an understanding of, and evaluate, management's process for assessing the effectiveness of the company's ICOFR
- ◆ Should evaluate whether management's process addressed the following:
 - Determining and documenting controls.
 - Evaluating which controls are significant/key.
 - Evaluating the design and operating effectiveness of the controls.
 - Determining which control deficiencies are of such a magnitude that they constitute significant deficiencies or material weaknesses.
 - Communicating findings to the external auditor and to others if applicable.
 - Determining whether findings are reasonable to support their assertion.

COSO, CobiT, Sarbanes-Oxley

Two control frameworks have been widely adopted by public companies subject to the requirements of the U.S. Sarbanes-Oxley Act of 2002:

- ◆ **COSO** Integrated Framework - the *Committee of Sponsoring Organizations*, released in 1992.
- ◆ **CobiT** - the IT Governance Institute's *Control Objectives for Information and Related Technology*.

COSO's target audience is management at large, CobiT is intended for management, users, and auditors (mostly IT auditors). Both COSO and CobiT view control as an entity-wide process, but CobiT specifically focuses on IT controls.

COSO, CobiT, Sarbanes-Oxley

The **COSO** framework states that internal control is a process - established by an entity's board of directors, management, and other personnel - designed to provide reasonable assurance regarding the achievement of stated objectives. COSO's control objectives cover effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. Its primary role is fiduciary.

CobiT approaches IT controls by looking at information - not just financial information - that is needed to support business requirements and the associated IT resources and processes. CobiT's role covers quality and security requirements in seven overlapping categories: effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

COSO Framework

The directions in Auditing Std. No. 2 are based on the internal control framework established by COSO.

Auditors are required only to address the financial reporting objective of COSO in an audit of internal control over financial reporting.

Five Components of Internal Control Framework



Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404

2. Scope of IT Controls

3. Key Considerations – Sampling Multiple Applications

4. Key Considerations – Baselining Legacy Systems

5. Key Considerations – Multi-location Scoping Criteria

6. Other Considerations

7. Evaluation of Control Deficiencies

8. IT Controls –Top Deficiencies

IT Control Activities

- ◆ IT General Controls
- ◆ Applications / Process Controls



IT Control Activities

IT General Controls (ITGC)

- ◆ Systems Development
- ◆ Change Management
- ◆ Computer and Data Center Operations
- ◆ Security, Physical and Logical (Access to Programs, and Data, and resources)

IT Control Activities

Application / Process Controls

- ◆ End-User Computing (spreadsheets, personal databases, ...)
- ◆ Authorization and Application Access
- ◆ Configuration and account mapping
- ◆ Exceptions and edit reports
- ◆ Interfaces and calculations

ITGC – System Development

- ◆ Methodology and monitoring
- ◆ Procedures and authorizations
- ◆ Testing procedures, including management and user acceptance
- ◆ Documentation requirements for system, users and controls
- ◆ Training requirements for new systems
- ◆ Post-implementation requirements including data integrity controls

ITGC – Change Management

- ◆ Change management procedures and authorizations
- ◆ Testing requirements for all changes prior to implementation
- ◆ Documentation requirements for system, user and control changes
- ◆ Access restrictions for change migrations
- ◆ Restricted and monitored production environment changes

ITGC – Computer and Data Center Operations

- ◆ Back-up procedures addressing critical systems and data
- ◆ Back-up restoration testing
- ◆ Offsite storage procedures and authorization controls
- ◆ Problem management procedures
- ◆ Job scheduling procedures and monitoring procedures

ITGC – Security, Physical & Logical

- ◆ Documented IT security policy and procedures, including appropriate compliance monitoring
- ◆ Logical and physical access to IT computing resources is appropriately restricted
- ◆ User accounts are added, modified and deleted in a timely manner
- ◆ Periodic review of user access rights and system permissions
- ◆ Appropriate segregation of duties exist within key processes

Applications / Process Controls

- ◆ End-User Computing.
- ◆ Authorization and Application Access.
- ◆ Configuration and Account Mapping (e.g. automatic mapping of GL transactions, recording of revenue and cost, 3-way matching, etc.).
- ◆ Exceptions and Edit reports.
- ◆ Interfaces and Calculations, accuracy & integrity.

Impact of ITGC on Process Controls

Example Scenario

- ◆ Control activity process: purchasing.
- ◆ Process / application control: purchasing clerk may only make purchases up to \$20,000 without additional approval.
- ◆ Process control is enabled by the purchasing system
- ◆ Purchasing system is dependent on proper functioning of IT general controls (four categories).
- ◆ Example IT general control: programmers cannot migrate changes directly into production.

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
- 3. Key Considerations – Sampling Multiple Applications**
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
7. Evaluation of Control Deficiencies
8. IT Controls – Top Deficiencies

Sampling Multiple Applications

- ◆ Q. If there are many applications, all different... does the auditor have to test them all, can auditor/company management group them in any way, can auditor/company management sample across a few, or do auditor/company management have to test them all.
- ◆ A. For any audit objective auditor/company management should determine whether there is a “common process” that applies to all applications (or platforms). If so, auditor/company management can and should sample across the process rather than retest for each application.
 - However, auditor/company management should do enough testing to validate that it truly is a common process.

Sampling Multiple Applications

Examples:

- Application security is administered using a common process for all user additions / changes.
- A common system development process is used for all applications even though there are different groups of programmers for different applications.
- A common change control process is used for all applications on a common platform even though they are resident in multiple data centers.

Sampling Multiple Applications

Examples:

- The company has multiple AS/400s that are all configured according to a common entity wide policy, and management has a process to review compliance with that configuration.
- A common process is used to backup & restore all or a large group of applications

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
- 4. Key Considerations – Baselining Legacy Systems**
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
7. Evaluation of Control Deficiencies
8. IT Controls – Top Deficiencies

Baselining Legacy Systems

Why does it need to be done?

- ◆ PCAOB Standard No. 2, paragraph 50 specifically requires that program development controls must be tested.
- ◆ The PCAOB has indicated, that existing systems are not grandfathered and program development controls must be performed, for all significant legacy systems in the first year.

Baselining Legacy Systems

What are the issues?

- ◆ How does management know the system works?
- ◆ How has the company documented they know it works?
- ◆ How has management tested or proved that the system works?

Baselining Legacy Systems

◆ For legacy systems/applications, management can create a baseline by:

- Providing adequate evidence of critical Program Development Controls, which at a minimum include system testing and documentation
- Also, management must provide evidence of adequate Program Change control from the implementation date going forward.

and/or by

- Providing adequate evidence that the system is performing as intended to verify that transactions and interfaces that impact the Financial Reporting are processed completely and accurately.

Baselining Legacy Systems

Other points to consider

- ◆ IT systems provided by major vendors have generally undergone testing, therefore the amount of testing required by management may be more limited and focused on customizations.
- ◆ Baselining also applies to spreadsheets and other end-user computing.
- ◆ If business process or application is outsourced, management still has to provide evidence system is working.

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
- 5. Key Considerations – Multi-location Scoping Criteria**
6. Other Considerations
7. Evaluation of Control Deficiencies
8. IT Controls – Top Deficiencies

Multi-location Scoping Criteria

When determining locations for testwork, the Standard No. 2's multi-location testing considerations include:

◆ Financially significant

- Is the location or business unit individually important?
- Are there specific significant risks?
- Are there locations or business units that are not important even when aggregated with others?
- Are there documented company-level controls over this group?

◆ Important when aggregated

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
- 6. Other Considerations**
7. Evaluation of Control Deficiencies
8. IT Controls – Top Deficiencies

Other Considerations

- ◆ **Auditor should assess the competence and objectivity of internal audit and/or others under the direction of management, by considering and documenting the following:**
 - Degree of independence, objectivity and Technical competence of individuals performing testing.
 - The actions of management on reports and recommendations from internal audit and how this is evidenced.
 - The due professional care of management, especially whether the work is adequately planned, supervised and reviewed .
 - How internal audit is organized, directed by management, and its communication methods.
 - Review of all internal audit reports issued during the period.

Other Considerations – Using the Work of Others

Examples of areas where use of work of others is generally limited:

- Controls over period-end financial reporting process
- Certain IT general controls on which the operating effectiveness of other controls depend.
- Controls over non-routine or non-systematic processes.
- Controls over significant balance sheet items based on judgments and estimates, significant accounts, processes or disclosures where risk of failure to operate effectively is assessed as high.
- Controls test on an interim basis that were ineffective and have been remedied by management.

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
- 7. Evaluation of Control Deficiencies**
8. IT Controls – Top Deficiencies

Control Deficiencies

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

Control Deficiencies

Design deficiency – when a control necessary to meet the control objective is missing or an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met.

Operation deficiency – when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

Evaluating Deficiencies - Framework

- ◆ A multi-firm group (Big 4 and others) developed and published a suggested framework for evaluating exceptions and deficiencies found from the evaluation of a company's internal control over financial reporting.
- ◆ The framework reflects the group's views and was developed to be consistent with PCAOB Auditing Standard No. 2 (AS2).
- ◆ The framework recognizes the requirement of AS2 to consider likelihood and magnitude in evaluating deficiencies.

Evaluating Deficiencies - Framework

- ◆ **For a control to function properly, it needs to be effective in both its design and operation**
- ◆ **If the design is ineffective to meet the control objective, the control is deficient**
- ◆ **If testing exceptions are found, management or the auditor first determines if the control is deficient**
- ◆ **Management as well as the auditor should evaluate the deficiency for severity unless the control deficiency is to be or has been remediated**

Evaluating Deficiencies - Management's Responsibilities

Management must evaluate deficiencies before the auditor and determine whether:

- ◆ **They are of the magnitude and likelihood of occurrence that they constitute significant deficiencies or material weaknesses.**
- ◆ **The system of internal control, taken as a whole, is operating effectively.**
- ◆ **Consider impact of deficiency on interim financial reporting as well as annual financial reporting.**
- ◆ **Consider and evaluate deficiencies in the aggregate.**

Management's Communication Requirement

Management is required to include its assessment of the effectiveness of the entity's internal control as of the end of the most recent fiscal year in its annual report

Evaluating Deficiencies – Evaluation of Likelihood

◆ Is it reasonably possible that an error could occur?

◆ Consider the following factors:

- The nature of the financial statement accounts, disclosures and assertions involved
- The susceptibility of the related assets or liabilities to loss or fraud
- The subjectivity, complexity or extent of judgment required to determine the related amounts involved
- The cause and frequency of known exceptions regarding the operating effectiveness of a particular control
- The interaction or relationship of the control with other controls
- The interaction of identified deficiencies
- The possible future consequences of the deficiency

Evaluating Deficiencies – Evaluation of Magnitude

- ◆ **Could the error be more than inconsequential (for a significant deficiency) or material to the financial statements (for a material weakness)?**

- ◆ **Consider the following factors:**
 - The financial statement amounts or totals of transactions exposed to the deficiency.
 - The volume of activity in the account or class of transactions exposed to the deficiency
 - The risk of potential misstatement may exceed recorded balances

Contents / Agenda

1. Overview of Sarbanes-Oxley (SOX) Section 404
2. Scope of IT Controls
3. Key Considerations – Sampling Multiple Applications
4. Key Considerations – Baselining Legacy Systems
5. Key Considerations – Multi-location Scoping Criteria
6. Other Considerations
7. Evaluation of Control Deficiencies
- 8. IT Controls –Top Deficiencies**

IT Controls – *Top Deficiencies*

The following are common deficiencies that have been identified by the company and auditor in this first year of SOX-404 testing...

- 1. Unidentified or unresolved segregation of duties issues.**
- 2. Programmer/Developer access to production business transactions.**
- 3. Large number of users with access to ‘Super’ or ‘Power’ User transactions in production.**
- 4. Terminated employees or departed consultants still have access.**

IT Controls – *Top Deficiencies*

- 5. Controls identified and tested are detective in nature rather than a balance of detective and preventive controls.**
- 6. Posting periods not restricted within GL application.**
- 7. Custom programs, tables, & interfaces unsecured.**
- 8. Procedures for manual processes do not exist.**
- 9. System documentation does not match actual process.**

Developer Access to Production Environment

- ◆ Very common among companies where small IT shops exist - not enough people for proper Segregation of Duties (SOD)
- ◆ Five ITGC Control Objectives could be violated by Developer Access to the Production Environment
- ◆ Deficiency impact is open to auditor judgment
- ◆ Compensating controls to reduce impact

Significant challenges some are experiencing

- Understanding of PCAOB scope
- Understanding of “what is key control?”
- Understanding of “what is gap?”
- Not having an enterprise wide policy for a process.
- Lack of sufficient evidence.
- Documenting what Business Owner would like to see, rather than documenting the process as it is.
- Test scripts not being executed properly by control owners.

Thank You

Questions ?