

A.I.S. Class 11: Outline

- Learning Objectives for Chapter 10
- Controls
- Misstatements
- Internal Control Structure
- Control Objectives and Audit Objectives
- COBIT
- Events and Event Risks
- Group Work for Chapter 10
- Mid-term Examination

Learning Objectives for Chapter 10

- After studying this chapter you should be able to:
 - ◆ provide a definition of controls
 - ◆ explain the concepts of exposure and reasonable assurance as they relate to controls
 - ◆ explain the difference between preventive, detective, and corrective controls
 - ◆ describe and discuss a number of risks that could be found in computer based systems
 - ◆ discuss the essence of Sarbanes-Oxley and its impact on internal controls
 - ◆ discuss Statement on Auditing Standards (SAS) No. 55 and 78 and their implications for controls in information systems
 - ◆ provide a basic distinction between general and application controls as categories of controls

Learning Objectives for Chapter 10

- ◆ describe general control procedures for database oriented systems environments
- ◆ describe application controls that can be incorporated into a database AIS
- ◆ indicate some control procedures that can be instituted only in on line database systems
- ◆ explain how entity integrity and referential integrity contribute to better control in a database AIS
- ◆ explain the hierarchical nature of the relationship between the control environment, the accounting system, general and application control procedures
- ◆ briefly describe the COBIT control framework released by the Information Systems Audit and Control Association

Controls

- Controls are mechanisms to prevent or detect errors and irregularities
- Risk is the likelihood that an information system will experience errors or irregularities
- Exposure is the amount of loss that could occur if a risk is realized
- Controls are designed to provide *reasonable assurance* that data are error free

Controls

- Preventive v. detective
 - ★ *Corrective procedures*
 - ◆ are corrective
 - ◆ but are not really controls
- Manual v. programmed
- General v. application
- Compensating controls
 - ★ *Controls in one place remediate absence of controls in others*
- Key controls
 - ★ *Subset of controls on which auditors plan to rely*

Misstatements

- Errors

- ★ unintentional mistakes

- Irregularities

- ★ intentional alteration or misstatement of data

- Fraud (defalcation)

- Management fraud

Exposures and Risks

■ Exposures may arise from

- ◆ Erroneous record keeping
- ◆ Unacceptable accounting
- ◆ Business interruption
- ◆ Erroneous management decisions
- ◆ Fraud and embezzlement
- ◆ Statutory sanctions
- ◆ Excessive costs
- ◆ Loss or destruction of assets
- ◆ Competitive disadvantage

Exposures and Risks

■ Risks

- ◆ Errors in data
- ◆ Irregularities in data
- ◆ Loss of data
- ◆ Natural disasters
- ◆ Computer crime

Internal Controls and Sarbanes-Oxley

- Sarbanes-Oxley Act 2002
 - ★ In response to Enron, World-Com, etc.
- Created Public Company Accounting Oversight Board (PCAOB)
 - ★ Overseen by SEC
- Previously, Statements of Auditing Standards (SAS) published by the AICPA's Auditing Standards Board
- Now, PCAOB has the right to adopt, amend, modify, repeal or reject auditing standards

Internal Controls and Sarbanes-Oxley

- Title I
 - ★ PCAOB regulates audits and auditors of public companies
- Title II
 - ★ Auditor independence provisions and audit committees
- Title III
 - ★ New responsibilities regarding financial reporting
- Title IV
 - ★ New disclosures

Internal Controls and Sarbanes-Oxley

- In April 2003, PCAOB asserted authority over auditing standards
- Existing standards were “grandfathered” until they can be replaced
- Four new standards have been issued so far
- Auditing Standard No 2:
 - ★ *An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With An Audit of Financial Statements*

Internal Controls and Sarbanes-Oxley

■ Sarbanes-Oxley Act Section 404

★ Management responsible for

- ◆ Establishing and maintaining adequate internal controls over *financial reporting*
- ◆ Assessment of the effectiveness of controls
- ◆ Documenting and testing internal controls over financial reporting and reporting their conclusions to the auditor

★ Auditors must attest and report on management's assertions regarding internal controls

- ◆ This significantly extends the amount of work that would previously have been required

Internal Controls and Sarbanes-Oxley

■ Sarbanes-Oxley Act Section 404

- ★ Last year, compliance for the first time was a huge expense for public companies and a huge logistical problem for auditor firms who were struggling to meet the demand
- ★ Soon even more (smaller) companies will be subject to Section 404!
- ★ Last year 11% of public companies capitalized at over \$75M disclosed control deficiencies
- ★ This represented 6-8% of firms audited by Big 4 and 15% of firms audited by Grant Thornton and BDO

Internal Controls and Sarbanes-Oxley

- Under the Act, COSO has been adopted by the SEC as the acceptable internal control framework
- COSO is already incorporated into existing auditing standards (SAS 55, etc.)
- Auditing of controls at Public Companies now ruled by Auditing Standard No 2

General Systems Model

- Every system has
 - ★ Inputs
 - ★ Processes
 - ★ Outputs
 - ★ Boundary
 - ★ Environment
- Control systems
 - ★ Sensors
 - ★ Standards
 - ★ Control comparisons
 - ★ Activating units

Internal Control Structure

■ SAS 55, COSO, SAS 78, SAS 94

★ Internal Control is a process effected by an entity's board of directors, and other personnel, that is designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- ◆ effectiveness and efficiency of operations
- ◆ reliability of financial reporting
- ◆ compliance with applicable laws and regulations

Internal Control Structure

- SAS 55, COSO, SAS 78
 - ★ Control Environment
 - ★ Management's Risk Assessment
 - ★ Information System and Communication
 - ★ Control Activities
 - ★ Monitoring

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

Management's Risk Assessment

- Risk assessment for financial reporting is the identification, analysis, and management of risks relevant to the preparation of financial statements that are fairly presented in conformity with GAAP

Risk Assessment

■ Risks may arise from

- ◆ Changes in the operating environment
- ◆ New personnel
- ◆ New or revamped information systems
- ◆ Rapid growth
- ◆ New technology
- ◆ New lines, products or activities
- ◆ Corporate restructuring
- ◆ Foreign operations
- ◆ Accounting pronouncements

Information System

- Procedures aimed at identifying, assembling, analyzing, classifying recording and reporting an entity's transactions
- Maintain accountability for the related assets and liabilities

Control Activities

- Policies and guidelines that management has established to provide reasonable assurance that specific entity objectives will be met
 - ★ Adequate separation of duties
 - ★ Proper authorization of transactions
 - ★ Adequate documents and records
 - ★ Physical control over assets and records
 - ★ Independent checks on performance

Control Activities

■ General control procedures

- ★ Organizational controls
- ★ Systems development and amendment
- ★ Hardware and systems software controls
- ★ Security and access controls
- ★ Operations controls
- ★ Data backup and recovery

Control Activities

■ Application control procedures

★ *Input controls*

- ◆ field tests
- ◆ range tests
- ◆ length tests
- ◆ validity tests
- ◆ valid combinations tests
- ◆ closed loop verification
- ◆ completeness tests
- ◆ prompting
- ◆ system generated data
- ◆ entity integrity
- ◆ referential integrity

Control Activities

■ Application control procedures

★ Processing controls

- ◆ internal label tests
- ◆ sequence checks
- ◆ control total verification

★ Output controls

★ User control procedures

Control Objectives

■ Completeness

- ★ All transactions that occurred are entered and accepted for processing

■ Accuracy

- ★ All transactions are recorded
 - ◆ at the correct amount
 - ◆ in the proper account
 - ◆ in the proper period

■ Validity

- ★ All recorded transactions
 - ◆ actually occurred
 - ◆ relate to the company
 - ◆ were approved / authorized

■ Restricted Access

- ★ Data is protected against unauthorized amendments

Monitoring

- A process that assesses the quality of internal control over time
- It involves assessment by appropriate personnel of the design and operation of controls on a timely basis and the taking of necessary action

COBIT

- **Control Objectives for Information and related Technology**
- **Information Systems Audit and Control Association**
- **Management “best practices”**
- **34 high level control objectives**
- **IT processes in four domains**
 - ★ **Planning & organization**
 - ★ **Acquisition & implementation**
 - ★ **Delivery & support**
 - ★ **Monitoring**

Events and Event Risks

- The risks considered in our professional standards, and the controls to mitigate them, are substantially aimed at safeguarding information processes dealing with
 - ★ Recording
 - ★ Maintaining
 - ★ Reporting
- Arguably, these risks and controls are of most importance to the accountant who is concerned with the quality of financial and management information

Events and Event Risks

- From the business perspective, however, it may be more important to ensure that we can avoid
 - ★ Business events occurring at the wrong time or sequence
 - ★ Business events occurring without proper authorization
 - ★ Business events involving the wrong internal agent
 - ★ Business events involving the wrong external agent
 - ★ Business events involving the wrong resource
 - ★ Business events involving the wrong amount of resource
 - ★ Business events occurring at the wrong location

Events and Event Risks

- You may find it helpful, therefore, to consider these event by event; e.g.,
 - ★ **Customer Order**
 - ◆ Accepting an order from an undesirable customer
 - ◆ Accepting an order for an unavailable product
 - ◆ Allowing an unauthorized person to take an order
 - ★ **Transferring goods from warehouse to shipping**
 - ◆ Moving goods without authorization
 - ◆ An unauthorized agent moving goods
 - ◆ Moving incorrect inventory or amount to shipping
 - ◆ Moving goods to an unauthorized location
 - ◆ Improper or inadequate physical safeguards over access to the inventory, fire or other disasters, and inventory counts

Events and Event Risks

- ★ **Shipping goods**

- ◆ An unauthorized person shipping the goods
- ◆ Having inventory stolen from the shipping area
- ◆ Shipping to the wrong customer or an unauthorized location
- ◆ Shipping the wrong product or amount
- ◆ Shipping without proper authorization
- ◆ Shipping poorly packaged products
- ◆ Selecting a poor carrier or route
- ◆ Losing sales because of untimely shipments

- ★ **Receiving customer payments**

- ◆ Theft of cash
- ◆ Failing to deposit cash into the company's bank accounts
- ◆ Lapping

Group Work for Chapter 10

- Discussion Questions
- Problems 6 & 7 for next class
- We will go over Chapter 9 problems then

Mid-Term Examination

■ Main features

- ★ 250 points
- ★ Five main sections
 - ◆ 30 or so multiple-choice questions (similar to quizzes) worth 3 points each
 - ◆ Some definitions & abbreviations (2 points each)
 - ◆ Short questions and problems including some flowcharting questions
 - ◆ An REA modeling problem (40 - 50 points)
 - ◆ A short essay (30 points)
- ★ 80 minutes total time: 8:10 – 9:30 next Wednesday night in Beck
- ★ Constrained by time not difficulty . . . 3 points per minute . . .
- ★ . . . so you will be penalized for turning in late