

A.I.S. Class 15: Outline

- Questions relating to REA
- Learning Objectives for Chapter 10
- Controls
- Misstatements
- Internal Control Structure
- Control Objectives and Audit Objectives
- COBIT
- Group Work for Chapter 10

Questions relating to REA



Mid-Term Review

■ How many people would plan to attend a Mid-Term Review at

- * 7:40 – 9:30 p.m.
- * Thursday, October 26
- * Beck Auditorium
- * Covering flowcharts, REA, Chapters 8 & 9

?

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 Statement on Auditing Standards (SAS) No. 55 and its 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
- Manual v. programmed
- General v. application
- Key controls
- Compensating controls

Misstatements

- Errors

- * unintentional mistakes

- Irregularities

- * intentional alteration or misstatement of data

- Fraud (defalcation)

- Management fraud

Exposures and Risks

■ Exposures

- ◆ 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

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

- * 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
- * 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

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

- Validity
- Completeness
- Timeliness
- Authorization
- Valuation
- Classification
- Posting and summarization

Audit Objectives

- Validity
- Completeness
- Cutoff
- Ownership
- Valuation
- Classification
- Detail tie-in
- Mechanical accuracy
- Disclosure

Management Assertions

- SAS 31 - five categories of assertions
 - * Existence or occurrence
 - * Completeness
 - * Rights and obligations
 - * Valuation or allocation
 - * Presentation and disclosure

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

Group Work for Chapter 10

- Discussion Questions
- Problems 6 & 7