RUTGERS

Rutgers Business School
Newark and New Brunswick

33:010:458
Accounting Information Systems

Dr. Peter R. Gillett

Associate Professor
Department of Accounting, Business Ethics and Information Systems
Rutgers Business School–Newark and New Brunswick

A.I.S. Class 10: Outline

- Learning Objectives for Chapter 10
- Controls
- Misstatements
- Internal Control Structure
- Control Objectives and Audit Objectives
- COBIT
- Events and Event Risks
- Group Project Internal Control Documentation
- Group Work for Chapter 10

Learning Objectives for Chapter 10

- After studying this chapter you should be able to:
  * provide a basic distinction between general and application controls as categories of controls
  * 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

Learning Objectives for Chapter 10

- After studying this chapter you should be able to:
  * 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
  - * Largely a matter of timing
    - Preventive - before anything CAN go wrong
    - Detective - afterwards, to assure that nothing HAS gone wrong
    - Need an appropriate balance of each
  - * Corrective procedures, discussed by Murthy & Groomer
    - are corrective
    - but are not really controls!
- Manual v. programmed
  - * Is the control exercised by a person or a computer program?

Controls

- General v. application
  - Does the control apply to all applications or is it specific to one in particular
- 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
- Five new standards have been issued so far
- Auditing Standard No 5 (replaced Auditing Standard No 2 in 2007):
  - An Audit of Internal Control Over Financial Reporting That Is Integrated 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
  * 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
  * Then even more (smaller) companies subject to Section 404!
  * Initially 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 an acceptable internal control framework
- COSO is already incorporated into previous auditing standards (SAS 55, etc.)
- Auditing of controls at Public Companies now ruled by Auditing Standard No 5, which references COSO

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, AS 5
  - 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, SAS 94, AS 5
  - * 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

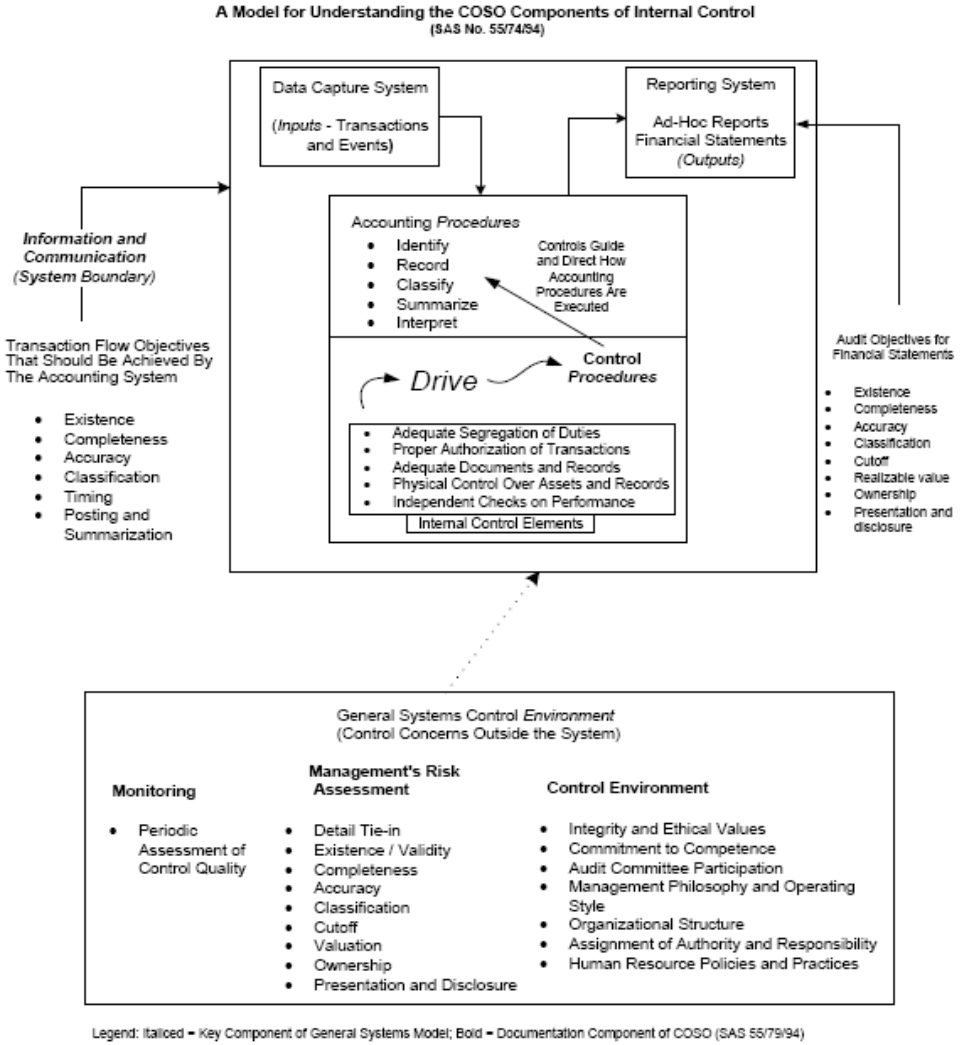
Control Activities

- 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 – batch systems
    - internal label tests
    - sequence checks
    - control total verification
  - * Output controls
  - * User control procedures

Accounting Information Systems



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
- 215 detailed control objectives
- IT processes in four domains
  * Planning & organization
  * Acquisition & implementation
  * Delivery & support
  * Monitoring & evaluation

COSO / COBIT

- COSO
  - Effectiveness
  - Efficiency
  - Reliability
  - Compliance
- COBIT
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability

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

Internal Control Documentation

- Group Project Internal Control Documentation
  - Based on a composite of actual documents used by accounting firms to record client's controls
  - Complete document includes six pages for General Controls which we shall not be using this year
  - In general, these four pages, covering application controls, need to be completed separately for each application, documenting controls over:
    - Input
    - Processing
    - Output
    - User
  - As many copies of each page as needed must be completed

Internal Control Documentation

- Group Project Internal Control Documentation
  - Each specific control activity must be documented, identifying:
    - The Type of Control (e.g., Range Test)
    - The specific Control Activity (e.g., Attempts to enter Hourly Rates < 0.00 or > 15.000 are rejected with an error message) in enough detail to be able to set them up in Microsoft ACCESS if necessary
    - Whether the control activity is Preventive or Detective
    - Whether the control activity is Manual or Programmed
    - Which Control Objective(s) the activity helps achieve
  - Good control may help achieve multiple Control Objectives
  - When the document is completed, it need to be reviewed to ensure that each Control Objective is appropriately covered, and that appropriate mixtures of Preventive and Detective controls, and Manual and Programmed controls, has been achieved

Group Work for Chapter 10

- Discussion Questions
- Problems 6 & 7 for next Monday