Accounting Information Systems

PRESENTED BY: EDGAR OTIENO

Lecture 7
Ethics Fraud & Internal Control and Auditing computerized financial systems

Ethics Fraud & Internal Control Objectives

- Broad issues pertaining to business ethics
- Ethical issues related to the use of information technology
- Distinguish between management fraud and employee fraud
- Common types of fraud schemes
- Objects and application of physical controls

Business Ethics

- Why should we be concerned about ethics in the business world?
- Ethics are needed when conflicts arise—the need to choose
- In business, conflicts may arise between:
  - employees
  - management
  - stakeholders
- Litigation

Business Ethics, cont ….

- **Business ethics** involves finding the answers to two questions:
- How do managers decide on what is right in conducting their business?
- Once managers have recognized what is right, how do they achieve it?

Four Main Areas of Business Ethics

Ethical Issues in Business

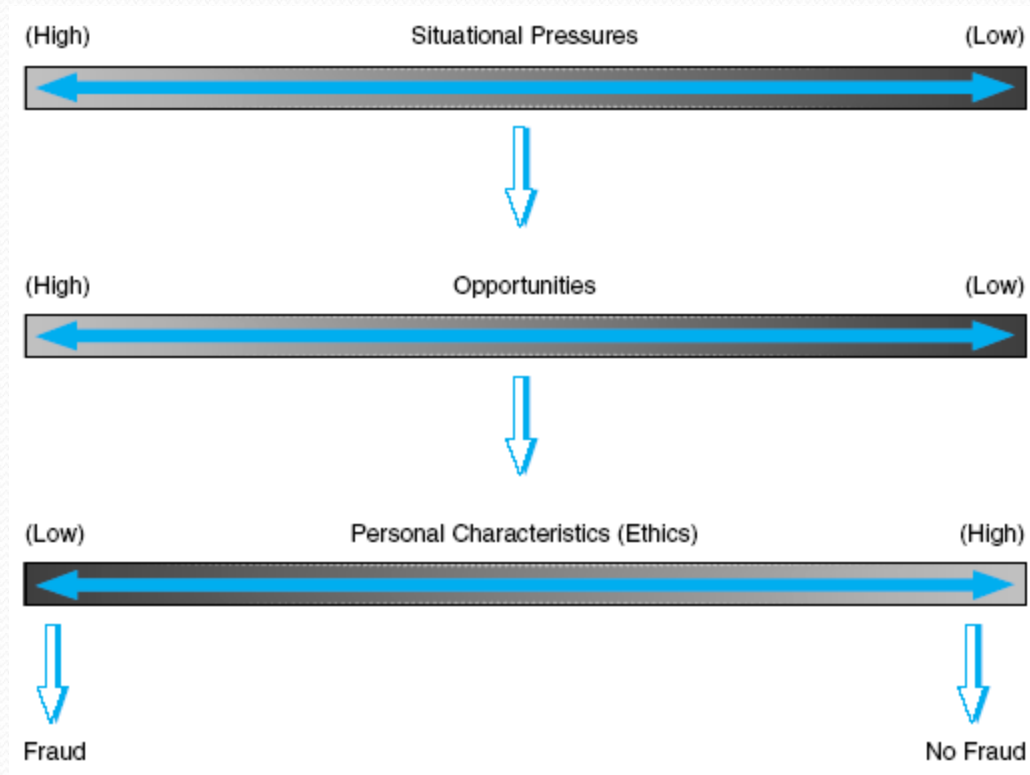|	
Equity	Executive Salaries Comparable Worth Product Pricing
Rights	Corporate Due Process Employee Health Screening Employee Privacy Sexual Harassment Diversity Equal Employment Opportunity Whistle-Blowing
Honesty	Employee and Management Conflicts of Interest Security of Organization Data and Records Misleading Advertising Questionable Business Practices in Foreign Countries Accurate Reporting of Shareholder Interests
Exercise of Corporate Power	Political Action Committees Workplace Safety Product Safety Environmental Issues Divestment of Interests Corporate Political Contributions Downsizing and Plant Closures

Computer Ethics

- Concerns the social impact of computer technology (hardware, software, and telecommunications).
- **What are the main computer ethics issues?**

  - Privacy
  - Security—accuracy and confidentiality
  - Ownership of property
  - Equity in access
  - Environmental issues
  - Artificial intelligence
  - Unemployment and displacement
  - Misuse of computer

Legal Definition of Fraud

- *False representation* - false statement or disclosure
- *Material fact* - a fact must be substantial in inducing someone to act
- *Intent to deceive* must exist
- The misrepresentation must have resulted in *justifiable reliance* upon information, which caused someone to act
- The misrepresentation must have caused *injury or loss*

Factors that Contribute to Fraud

	Situational Pressures	
(High)		(Low)

	Opportunities	
(High)		(Low)

	Personal Characteristics (Ethics)	
(Low)		(High)

Fraud

No Fraud

Employee Fraud

- Committed by **non-management personnel**
- Usually consists of: an employee taking cash or other assets for personal gain by circumventing a company's system of internal controls

Management Fraud

- Perpetrated at levels of management above the one to which internal control structure relates
- Frequently involves using financial statements to create an illusion that an entity is more healthy and prosperous than it actually is
- Involves misappropriation of assets, it frequently is shrouded in a maze of complex business transactions

Fraud Schemes

- Three categories of fraud schemes according to the Association of Certified Fraud Examiners:

    A. fraudulent statements

    B. corruption

    C. asset misappropriation

A. Fraudulent Statements

- Misstating the financial statements to make the copy appear better than it is
- Usually occurs as management fraud
- May be tied to focus on short-term financial measures for success
- May also be related to management bonus packages being tied to financial statements

B. Corruption

- Examples:
  - bribery
  - illegal gratuities
  - conflicts of interest
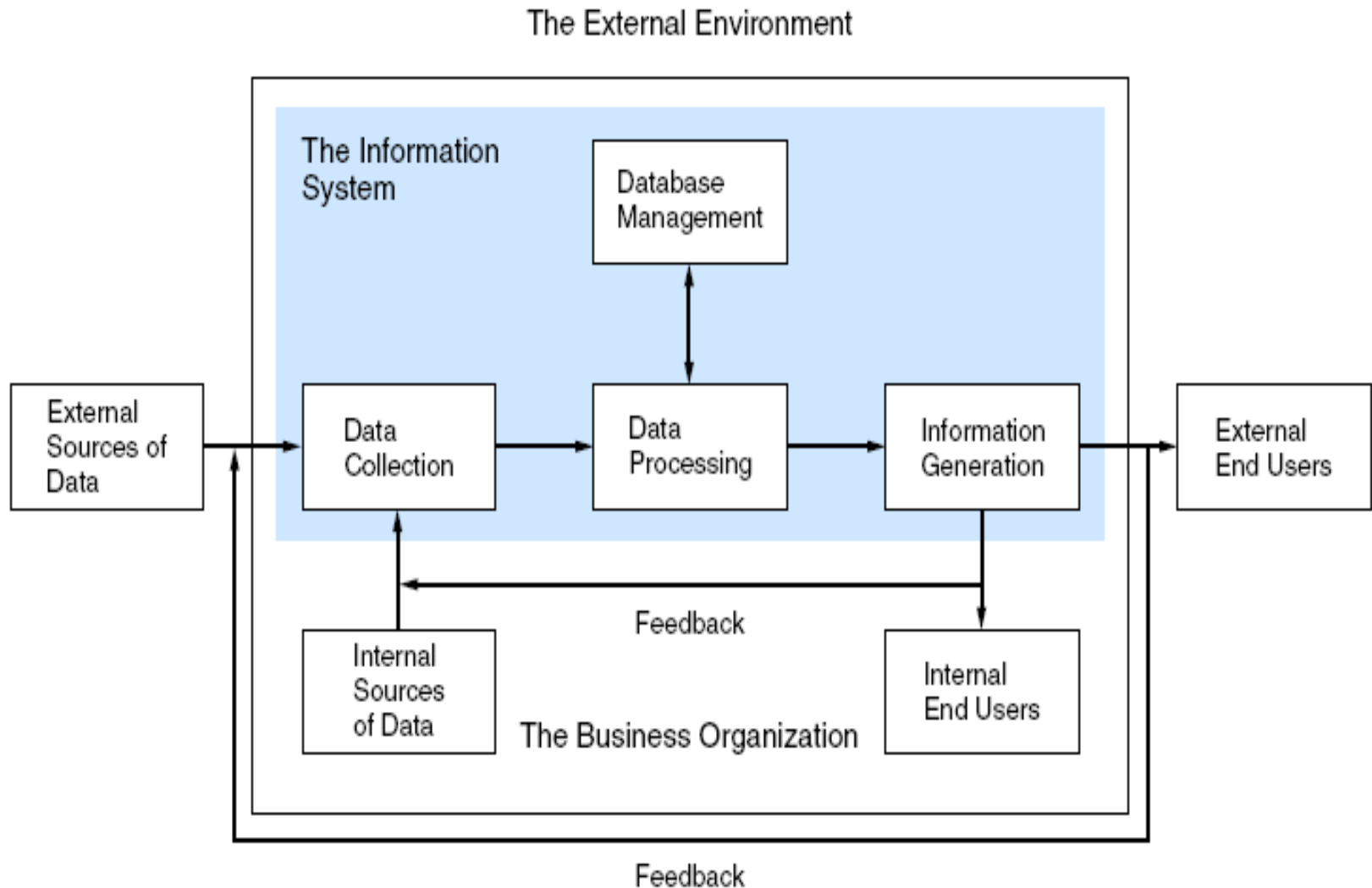 - economic extortion

C. Asset Misappropriation

- Most common type of fraud and often occurs as employee fraud
- Examples:
  - making charges to expense accounts to cover theft of asset (especially cash)
  - *lapping*: using customer's cheque from one account to cover theft from a different account
  - *transaction fraud*: deleting, altering, or adding false transactions to steal assets

Computer Fraud Schemes

- Theft, misuse, or misappropriation of assets by altering computer-readable records and files
- Theft, misuse, or misappropriation of assets by altering logic of computer software
- Theft or illegal use of computer-readable information
- Theft, corruption, illegal copying or intentional destruction of software
- Theft, misuse, or misappropriation of computer hardware

Using the general IS model, explain how fraud can occur at the different stages of information processing?

The External Environment

The Information System

Database Management

External Sources of Data → Data Collection → Data Processing → Information Generation → External End Users

Feedback

Internal Sources of Data

The Business Organization

Internal End Users

Feedback

Data Collection Fraud

- This aspect of the system is the **most vulnerable** because it is relatively easy to change data as it is being entered into the system.

- Also, the GIGO (garbage in, garbage out) principle reminds us that if the input data is inaccurate, processing will result in inaccurate output.

Data Processing Fraud

Program Frauds

- altering programs to allow illegal access to and/or manipulation of data files
- destroying programs with a virus

Operations Frauds

- misuse of company computer resources, such as using the computer for personal business

Database Management Fraud

- Altering, deleting, corrupting, destroying, or stealing an organization's data
- Oftentimes conducted by disgruntled or ex-employee

Information Generation Fraud

Stealing, misdirecting, or misusing computer output

<u>Scavenging</u>

- searching through the trash cans on the computer center for discarded output (the output should be shredded, but frequently is not)
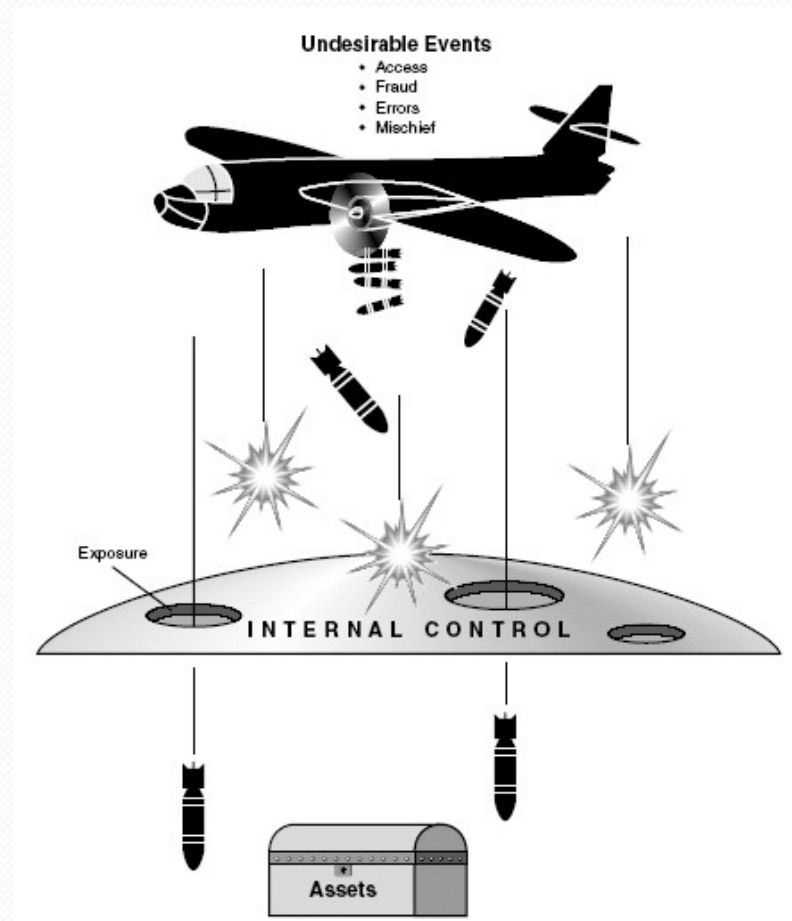
Limitations of Internal Controls

- Possibility of honest errors
- Circumvention via collusion
- Management override
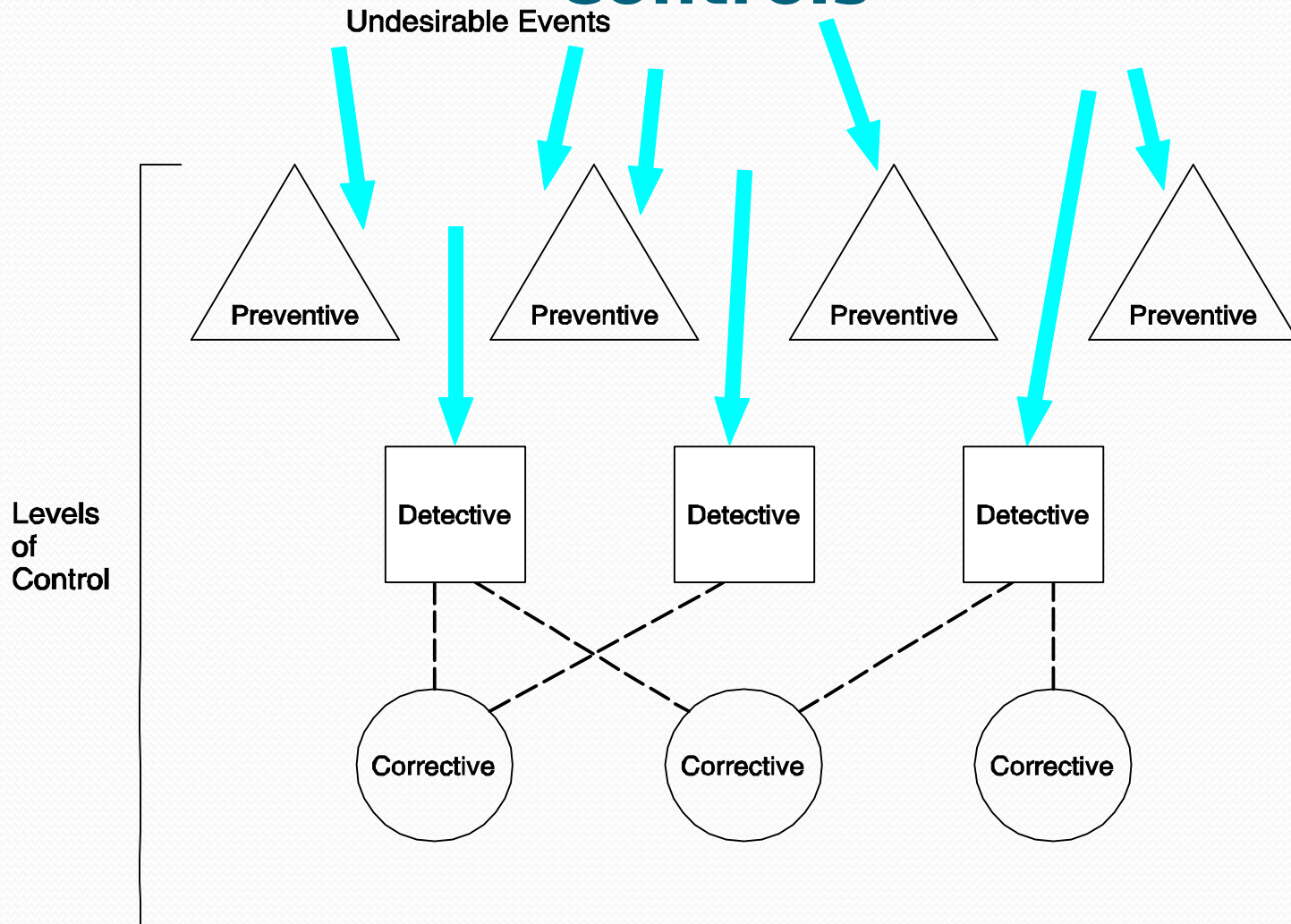- Changing conditions--especially in companies with high growth

Exposures of Weak Internal Controls (Risk)

- **Destruction** of an asset
- **Theft** of an asset
- **Corruption** of information
- **Disruption** of the information system

The Internal Controls Shield

Preventive, Detective, and Corrective Controls

Two Types of IT Controls

- **General controls—**pertain to the entity-wide computer environment
  - Examples: controls over the data center, organization databases, systems development, and program maintenance
- **Application controls—**ensure the integrity of specific systems
  - Examples: controls over sales order processing, accounts payable, and payroll applications

AUDITING COMPUTER SYSTEMS

Auditing of computerised systems especially where they are distributed may be complex in the following aspects:-

- Cost – Auditing of computerised may be expensive especially where CAATs are used.

- Data stored in magnetic files may be subject to manipulation without leaving any visible trail.

- The auditor may not be able to visit all the company branches because of their location and therefore he may rely on sampling which sometimes may increase his potential liability.

- Loss of audit trail, the auditor may not be able to trace totals and balances of individual transactions through the system from source to completion and vice versa, this because some of the intermediary records may be missing.

AUDIT APPROACH IN COMPUTERISED ENV.

Auditing through the computer

- This is where the auditor is expected to have the knowledge of inputs, processing and output technology. He studies the equipment, processing and controls incorporated to ensure that all transactions are accounted for. The emphasis of auditing through the computer is to ensure existence and sufficiency of internal control system in processing. The reasons for auditing through the computer are:-
    - Loss of audit trail
    - There are too many transactions
    - There are sophisticated processing program

Advantages

- It uses the computer as the auditing tool and hence increase the auditors knowledge of the computer.
- There are thorough audit procedures which ensure completeness, accuracy and validity of financial information.
- It is the only auditing method which can be used by large organisation.
- Faster and easier to use.

Auditing around the computer (black-box auditing)

- This is where the auditor is assumed to be computer illiterate. He can only evaluate manual sample and compares it with the computer output. If both are consistent or correct processing is assumed to have been correct also.

- Advantages
    - There is no need for knowledge on computer technology
    - Its the only method used by small companies

AUDIT TRAIL

- This is tracing of totals and balances of individual translations through a system from source to completion or vice versa. The need for audit trail is vital for two reasons:-
- To identify errors
- To detect frauds

COMPUTER ASSITED AUDIT TECHNIQUES (CAATS)

- These are techniques which help the auditor to overcome loss of audit trail. They also reduce the chances of errors during auditing and speed up audit examination. CAATs normally come in form of audit packages.

IMPORTANCE OF CAATS

- To locate errors and potential fraud by comparing and analysing user criteria.
- They can be used to re-calculate and verify balance i.e. as a means of getting audit evidence.
- To identify control issues and ensure compliance with standards.
- To age and analyse accounts receivables, payables and any other business transactions.
- To test for unauthorised employee, or supplier relationships.
- To automate repetitive tasks by creating automised application software.
- To identify trends and pinpoint exceptions and potential areas of audit trail.
- In using CAATs, the auditor may need to consider the risk element, time and the nature of internal control system.

TYPES OF CAATS

a)Use of Test data

- This is inputting some data and processing it inorder to test processing data in the way it should be. The auditor may enter sample data and compare the expected results with actual results.

b)Audit interrogation software

- This software interrogates all the stages of transactions in a computerised system. He comes up with the programs and uses them to process the data that has been collected by the client. The auditor must take care not to rely too much on this software because it can hinder this creativity.

c)Embedded audit facilities.

- This allows a continuous review of the data recorded and treated by the systems. The embedded facility has a monitory system over the enterprises accounting system.

Factors affecting choice of CAATS

- Cost
- Expertise
- Application area
- Features available on the CAATs