Threats, Fraud, and Internal Controls

1

Threats to Accounting Information Systems

- A **threat** is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm: This include
- *software errors and equipment malfunctions*
  - hardware failures
  - power outages and fluctuations
  - undetected data transmission errors

7-2

Threats to Accounting Information Systems

- *unintentional acts*
  - accidents caused by human carelessness
  - innocent errors of omissions
  - lost or misplaced data
  - logic errors
  - systems that do not meet company needs

Threats to Accounting Information Systems

- *intentional acts*
  - sabotage
  - computer fraud
  - Embezzlement

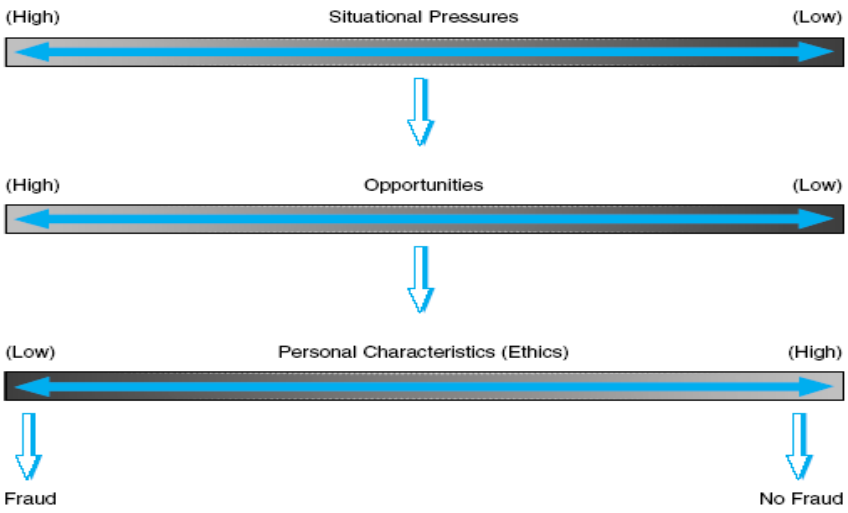
Others Types of Threats

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***

5

Factors that Contribute to Fraud



6

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

7

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.

8

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

9

Database Management Fraud

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

10

Information Generation Fraud

Stealing, misdirecting, or misusing computer output

Scavenging

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

11

Why AIS threats are increasing

- There are computers and servers everywhere, and information is available to an unprecedented number of workers.
- Distributed computer networks make data available to many users, and these networks are harder to control than centralized mainframe systems.
- Wide area networks are giving customers and suppliers access to each other's systems and data, making confidentiality a major concern.
- Wireless Technology

12

Why AIS threats are increasing

- Historically, many organizations have not adequately protected their data due to one or more of the following reasons:
  - Computer control problems are often underestimated and downplayed.
  - Control implications of moving from centralized, host-based computer systems to those of a networked system or Internet-based system are not always fully understood.
  - Companies have not realized that data is a strategic resource and that data security must be a strategic requirement.
  - Productivity and cost pressures may motivate management to forego time-consuming control measures.

Internal controls and AIS

Internal Controls

Internal control is the plan of organization and the methods a business uses to safeguard assets, provide accurate and reliable information, promote and improve operational efficiency, and encourage adherence to prescribed managerial policies.

A Primary Objective of an AIS

- Is to control the organization so the organization can achieve its objectives
- Management expects accountants to:
  - Take a proactive approach to eliminating system threats.
  - Detect, correct, and recover from threats when they occur.

Internal Controls

- Processes implemented to provide assurance that the following objectives are achieved:
  - Safeguard assets/data
  - Maintain sufficient records
  - Provide accurate and reliable information
  - Prepare financial reports according to established criteria
  - Promote and improve operational efficiency
  - Encourage adherence with management policies
  - Comply with laws and regulations

17

Internal Control Classifications

- The specific control procedures used in the internal control and management control systems may be classified using the following four internal control classifications:
  1. Preventive, detective, and corrective controls
  2. General and application controls
  3. Administrative and accounting controls
  4. Input, processing, and output controls

7-18

Functions of Internal Controls

- Preventive controls
  - Deter problems from occurring
- Detective controls
  - Discover problems that are not prevented
- Corrective controls
  - Identify and correct problems; correct and recover from the problems

19

Internal Control

- Preventive Control examples
  - Hire qualified personnel
  - Segregation of duties
  - Chart of accounts
  - Physical access controls
    - Assets
    - information
  - Employee training

20

Internal Control

- Detective Control examples
  - Preparing bank reconciliations
  - Log analysis
  - Fraud hotline
  - Prepare monthly trial balance

21

Internal Control

- Correctives Control examples
  - Back up copies of master and transaction files
  - Adequate insurance
  - Resubmission of transactions for subsequent processing
  - Correction of data entry errors

22

Internal Control

- Internal control is a ***process*** because:
  - It permeates an organization's operating activities.
  - It is an integral part of basic management activities.
- Internal control provides **reasonable**, rather than absolute, assurance, because complete assurance is difficult or impossible to achieve and prohibitively expensive.

23

Two Types of IT Controls

- **General controls/Physical Controls —**pertain to the entitywide 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

24

Six Types of Physical Controls

- Transaction Authorization
- Segregation of Duties
- Supervision
- Accounting Records
- Access Control
- Independent Verification

25

Physical Controls

Transaction Authorization

- used to ensure that employees are carrying out only authorized transactions
- *general* (everyday procedures) or *specific* (non-routine transactions) authorizations

26

Physical Controls

Segregation of Duties

- In manual systems, separation between:
  - *authorizing and processing a transaction*
  - *custody and recordkeeping of the asset*
  - *subtasks*
- In computerized systems, separation between:
  - *program coding*
  - *program processing*
  - *program maintenance*

27

Physical Controls

Supervision

- a compensation for lack of segregation; some may be built into computer systems

Accounting Records

- provide an audit trail

28

Physical Controls

Access Controls

- help to safeguard assets by restricting physical access to them

Independent Verification

- reviewing batch totals or reconciling subsidiary accounts with control accounts

29

Physical Controls in IT Contexts

Transaction Authorization

- The rules are often embedded within computer programs.
  - EDI/JIT: automated re-ordering of inventory without human intervention

30

Physical Controls in IT Contexts

Segregation of Duties

- A computer program may perform many tasks that are deemed incompatible.
- Thus the crucial need to separate program development, program operations, and program maintenance.

31

Physical Controls in IT Contexts

Supervision

- The ability to assess competent employees becomes more challenging due to the greater technical knowledge required.

32

Physical Controls in IT Contexts

Accounting Records

- ledger accounts and sometimes source documents are kept magnetically
  - no audit trail is readily apparent

33

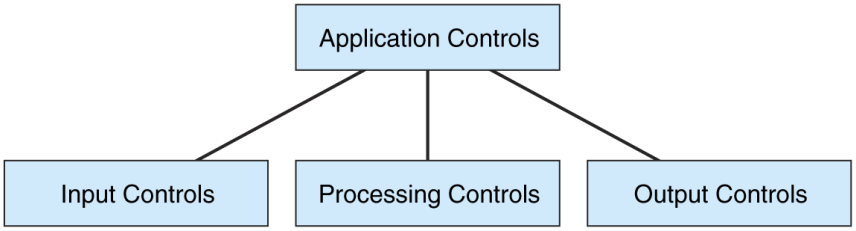
Physical Controls in IT Contexts

Access Control

- Data consolidation exposes the organization to computer fraud and excessive losses from disaster.

34

Application Controls for Transaction Processing



Application Controls for Transaction Processing

- **Application controls are designed to**
  - **prevent,**
  - **detect, and**
  - **correct errors and irregularities**

  in transactions in
  - **the input**
  - **processing**
  - **the output stages of data processing**

Input Controls

Input controls attempt to ensure the

- **validity**
- **accuracy**
- **completeness of the data entered into an AIS**

The categories of input controls include

- **observation, recording, and transcription of data**
- **edit tests**
- **additional input controls**

Observation, Recording, and Transcription of Data

The observation control procedures to assist in collecting data are

- **feedback mechanism**
- **dual observation**
- **point-of-sale (POS) devices**
- **preprinted recording forms**

Data Transcription

- **Data transcription**
  - **the preparation of data for computerized processing**
- ***Preformatted screens***
  - **Make the electronic version look like the printed version**

Edit Tests

Input validation routines (edit programs)

- **check the validity**
- **check the accuracy**

after the data have been

- **entered, and**
- **recorded on a machine-readable file of input data**

Edit Tests

Edit tests

- **examine selected fields of *input data* and**
- **reject those transactions whose data fields do not meet the pre-established standards of data quality**

Real-time systems use edit checks during data-entry.

Examples of Edit Tests

The following are the tests for copy editing

- **Numeric field**
- **Alphabetic field**
- **Alphanumeric field**
- **Valid code**
- **Reasonableness**
- **Sign**
- **Completeness**
- **Sequence**
- **Consistency**

Processing Controls

- ***Processing controls*** **focus on the manipulation of accounting data after they are input to the computer system.**
- **Key objective is a clear audit trail**
- **Processing controls are of two kinds:**
  - **Data-access controls**
  - **Data manipulation controls**

Data-Access Control Totals

Some common processing control procedures are

- **batch control total**
- **financial control total**
- **nonfinancial control total**
- **hash total**
- **record count**

Data Manipulation Controls

Once data has been validated by earlier portions of data processing, they usually must be *manipulated* in some way to produce useful output.

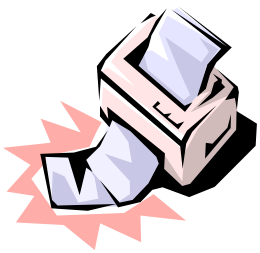
Data manipulation controls include:

- **Software documentation, i.e. flow charts and diagrams**
- **Compiler**
- **Test Data**

Output Controls

The objectives of output controls is to ensure

- **validity**
- **accuracy**
- **completeness**



Two major types of output application controls are

- **validating processing results by**
  - ***Activity (or proof) listings***

Output Controls

- **regulating the distribution and use of printed output through**
  - ***Forms***
  - ***Prenumbered forms***
  - ***authorized distribution list***
  - ***Shredding* sensitive documents**

Control Frameworks

- COBIT
  - Framework for IT control
- COSO
  - Framework for enterprise internal controls (control-based approach)
- COSO-ERM
  - Expands COSO framework taking a risk-based approach

48