KAMPALA INTERNATIONAL UNIVERSITY UGANDA

COURSE MODULE – ACCOUNTING INFORMATION SYSTEM

Faculty	**:**	**MBA**
Semester	**:**	**2:1**
Session	**:**	**DAY/WEEKEND**
Academic Year	**:**	**2020-2021**
College	**:**	**College of Economics and Management**
Department	**:**	**Accounting and Finance**
Subject Code & Title	**:**	**MBAFA 7305 Accounting Information System**
Lecturing Hours	**:**	**3 Hours Per Week**
Subject Instructor	**:**	**Dr. Omweno N. Enock**
Email address	**:**	**oenock@kiu.ac.ug**
Phone	**:**	**+254792652044/0774756286**

PURPOSE OF COURSE

Accounting is arguably one of the earliest applications of information system in business. Accountants need solid. Information system knowledge and skills in order to provide better information for the business decision making, a central feature of accounting in today's business world is the interaction of accounting. Professionals with computer based information systems. As primary users of information systems in organizations, accountants must participate in their design and implementation; and understand their operation.

Expected Learning Outcomes

By the end of the course unit students should be able to:

- Identify key issues associated with the application of the information systems for accounting and business decision making.
- Describe the core business process and understand how these processes are implemented in AIS.
- Discuss the risks and controls associated with business process and AIS
- Discuss the basic knowledge of how accounting information systems function in today's business environment.

- Explain the issues in information systems

UNIT 1

1.0 INTRODUCTION TO ACCOUNTING INFORMATION SYSTEMS

Aims of the study

At the end of the study, students should be able to:

i. Know the components of AIS
ii. Know Business Process and AIS
iii. Understand primary information flows within the business environment
iv. Learn accounting information systems and management information systems
v. Understand the general model for information systems
vi. Understand the Financial transactions from non-financial transactions
vii. Learn the functional areas of a business
viii. Understand two main stages in the evolution of information systems
ix. Learn the three roles of accountants in an information system

1.1 Introduction

Before understanding the concept of Accounting Information System, we all are aware of the general idea about the Accounting and Information System distinctively that the former is the language of business and the latter is a system composed of people and computers that processes or interprets information. In a broader sense, accounting can be explained as, “the principal way of organizing and reporting financial information. It has been called the language of business. The accounting system is used to identify, analyse, measure, record, summarize, and communicate relevant economic information to interested parties.”Information System can be explained as, “it is a system composed of people and computers that processes or interprets information. The term is also sometimes used in more restricted senses to refer to only the software used to run a computerized database or to refer to only a computer system.”But for an Information System, one must require data to process it into proper categorized information when needed. Therefore, ***Data*** are raw facts and figures that are processed to produce information.

Information is data that have been processed and are meaningful and useful to users. The terms meaningful and useful are value-laden terms and usually subsume other qualities such as timeliness, relevance, reliability, consistency, comparability, etc. ”What are the components that really make an information system work? Take example of IPO (input, process and output) and how this system works.

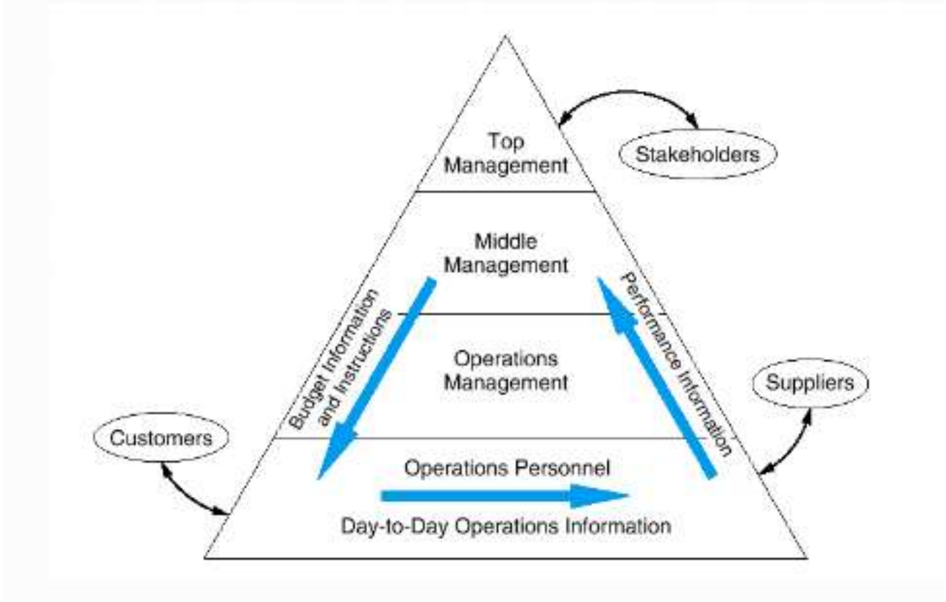
Input is anything we wish to embed in a system for some type of use. A variety of sources are used to input: keyboard, scanner, microphone, mouse, even another computer. What we input has a purpose or an objective that can be termed as a data-but until and unless it is processed and generated in some form of output, it is technically of no use or purpose to be achieved. Processing takes place in the internal parts of the computer system. It is the act of taking inputted data and processing or converting it into something useful. What we typically see on the screen in today's computer world (known as ***What You See Is What You Get*** or in short as WYSIWYG) is the result of our input being processed by some logical program so we can have the required output: an English paper, an edited photograph, ‘this video you're watching’. Output or the processed information in a usable format comes in various forms: monitor or printer for visual work, a speaker for audio. Sometimes our output is short-term, such as printing a photo, and sometimes what we work on needs to be kept around for a while. That's where storage comes in.

Storage is the term used to indicate that we will be saving data for a period of time. We store for many reasons: for future reference; to prevent full loss of data; because we forget to purge. But, storage is vital. There are several mediums on which we can keep output and processed data: a hard disk, a USB drive, a CD. Feedback is where the output from a system is fed back into the system in order to influence the input.

For example, when you try to withdraw too much money from your account at an ATM a warning on the screen will advise you that it isn't possible and will suggest that you try to withdraw a smaller amount. This is a type of feedback because it is trying to influence your input.

In short let us take some few simple definitions in relation to AIS before you proceed to business process.

1.1.1 INTERNAL AND EXTERNAL INFORMATION FLOW



1.1.1. a. Internal Information Flows

i. Horizontal flows of information used primarily at the operations level to capture transaction and operations data

ii. Vertical flows of information

- Downward flows — instructions, quotas, and budgets
- Upward flows — aggregated transaction and operations data

1.1.1. b. Information Requirements

Each user group has unique information requirements. The higher the level of the organization, the greater the need for more aggregated information and less need for detail.

1.1.1. c. Information in Business

Information is a business resource that: Needs to be appropriately managed. Is vital to the survival of contemporary businesses.

1.1.1. d. What is a System?

A group of interrelated multiple components or subsystems that serve a common purpose. A **system** is called a subsystem when it is viewed as a component of a larger system. A **subsystem** is considered a system when it is the focus of attention.

1.1.1. e. What is an Information System?

An information system is the set of formal procedures by which data are collected, processed into information, and distributed to users.

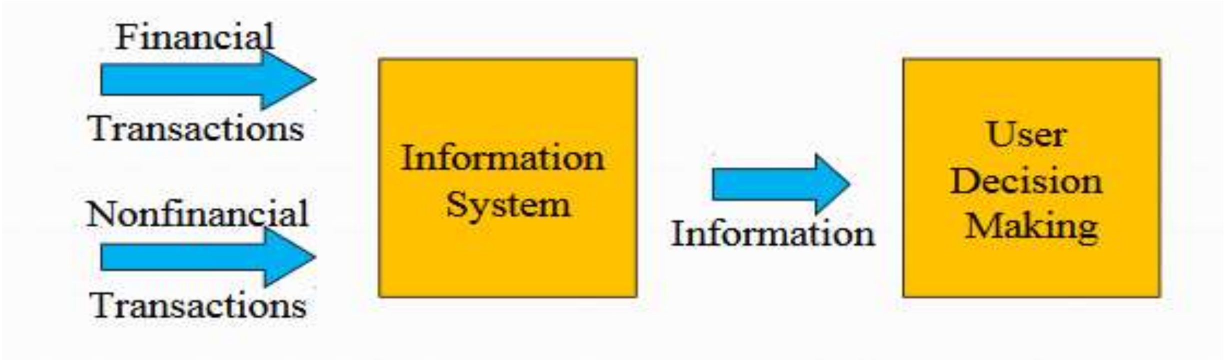
1.1.2 Transactions

A transaction is a business event.

Financial transactions - economic events that affect the assets and equities of the organization e.g., purchase of an airline ticket

Nonfinancial transactions - all *other* events processed by the organization’s information system e.g., an airline reservation — no commitment by the customer.

Transactions:



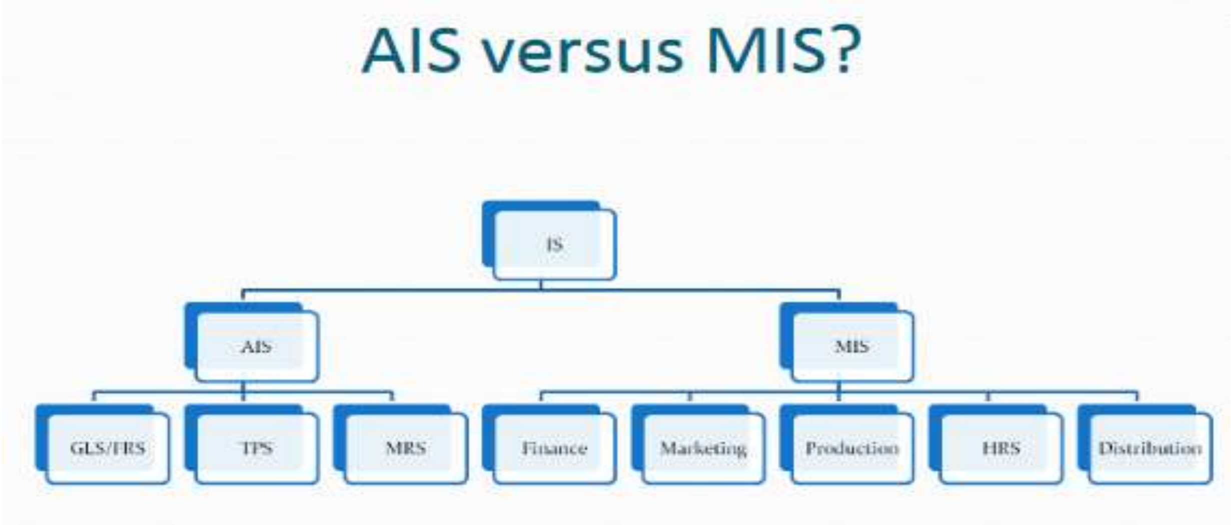
1.1.3 What is Accounting Information Systems?

Accounting is an information system. It identifies, collects, processes, and communicates economic information about a firm using a wide variety of technologies. It captures and records the financial effects of the firm’s transactions. It distributes transaction information to operations personnel to coordinate many key tasks.

AIS VERSUS MIS

Accounting Information Systems (AIS) process – is a financial transactions; e.g., sale of goods and nonfinancial transactions that directly affect the processing of financial transactions; e.g., addition of newly approved vendors.

1.1.3 Management Information Systems (MIS) process – A nonfinancial transactions that are not normally processed by traditional AIS; e.g., tracking customer complaints



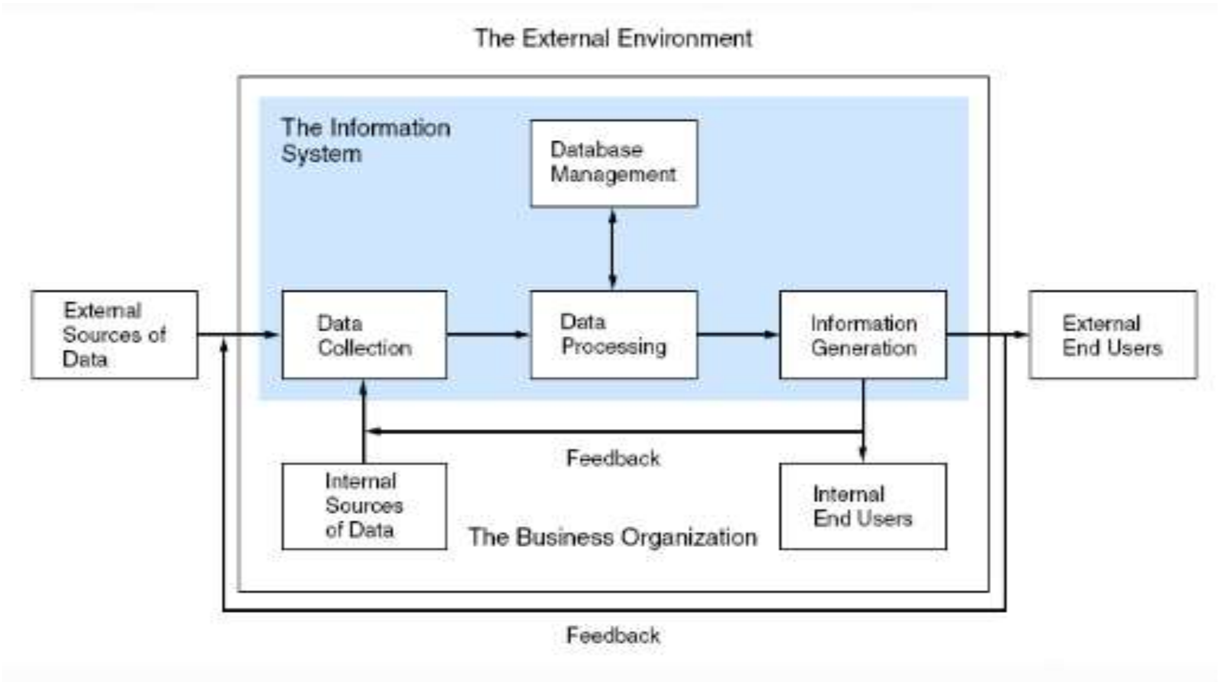
AIS Subsystems

Transaction processing system (TPS) - supports daily business operations

General Ledger/ Financial Reporting System (GL/FRS) - produces financial statements and reports

Management Reporting System (MRS) - produces special-purpose reports for internal use.

1.1.4 THE GENERAL AIS MODEL



1.1.5 DATA SOURCES

Data sources are financial transactions that enter the information system from internal and external sources.

- External financial transactions are the most common source of data for most organizations. E.g., sale of goods and services, purchase of inventory, receipt of cash, and disbursement of cash (including payroll).
- Internal financial transactions involve the exchange or movement of resources within the organization. E.g., movement of raw materials into work-in-process (WIP), application of labor and overhead to WIP, transfer of WIP into finished goods inventory, and depreciation of equipment.

Transforming the Data into Information

Functions for transforming data into information according to the general AIS model:

1. Data Collection 2. Data Processing 3. Data Management 4. Information Generation.

1. Data Collection can be done by Capturing transaction data, Recording data onto forms, Validating and editing the data

2. Data Processing. Classifying, Transcribing, Sorting, Batching, Merging, Calculating, Summarizing and Comparing.

3. Data Management. Storing, Retrieving, Deleting

4. Information Generation. Compiling, Arranging, Formatting, Presenting.

Characteristics of Useful Information

Regardless of physical form or technology, useful information has the following characteristics:

i. **Relevance**: serves a purpose
ii. **Timeliness**: no older than the time period of the action it supports
iii. **Accuracy**: free from material errors
iv. **Completeness**: all information essential to a decision or task is present
v. **Summarization**: aggregated in accordance with the user’s needs.

Information System Objectives in a Business Context

The goal of an information system is to support the stewardship function of management, management decision making, the firm's day-to-day operations

1.1.6 Organizational Structure

The structure of an organization helps to allocate, responsibility, authority, accountability. Segmenting by business function is a very common method of organizing.

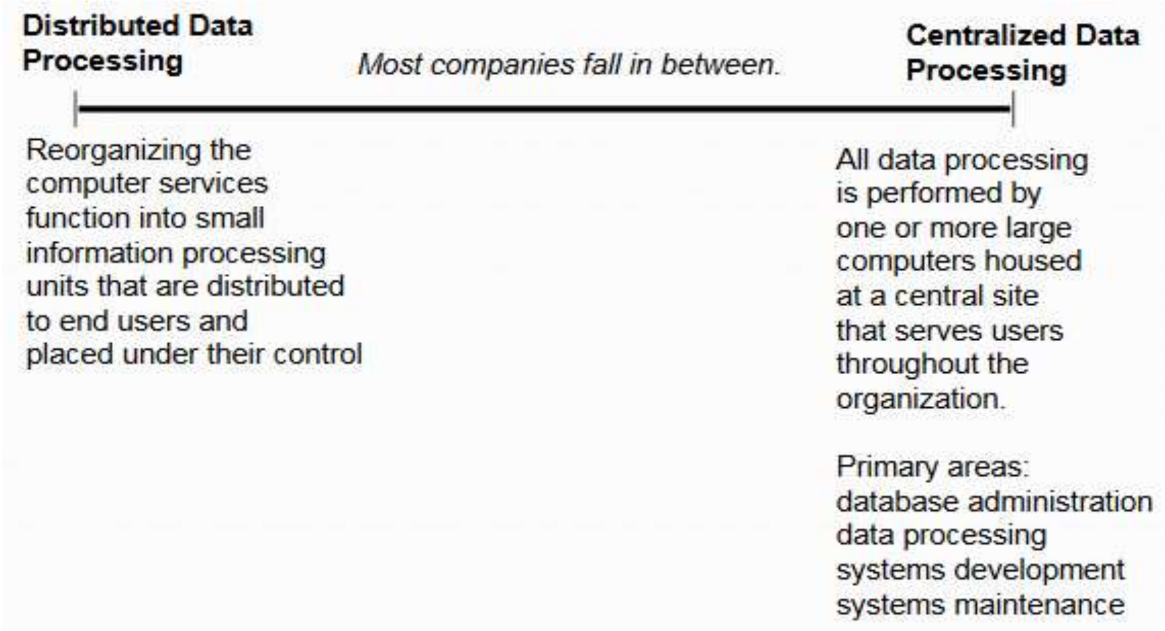
Functional Areas

a. Inventory/Materials Management - purchasing, receiving and stores
b. Production - production planning, quality control, and maintenance
c. Marketing
d. Distribution
e. Personnel
f. Finance
g. Accounting
h. Computer Services

1.1.7 Accounting Independence

Information reliability requires accounting independence. Accounting activities must be separate and independent of the functional areas maintaining resources. Accounting supports these functions with information but does not actively participate. Decisions makers in these functions require that such vital information be supplied by an independent source to ensure its integrity.

Computer Service Function



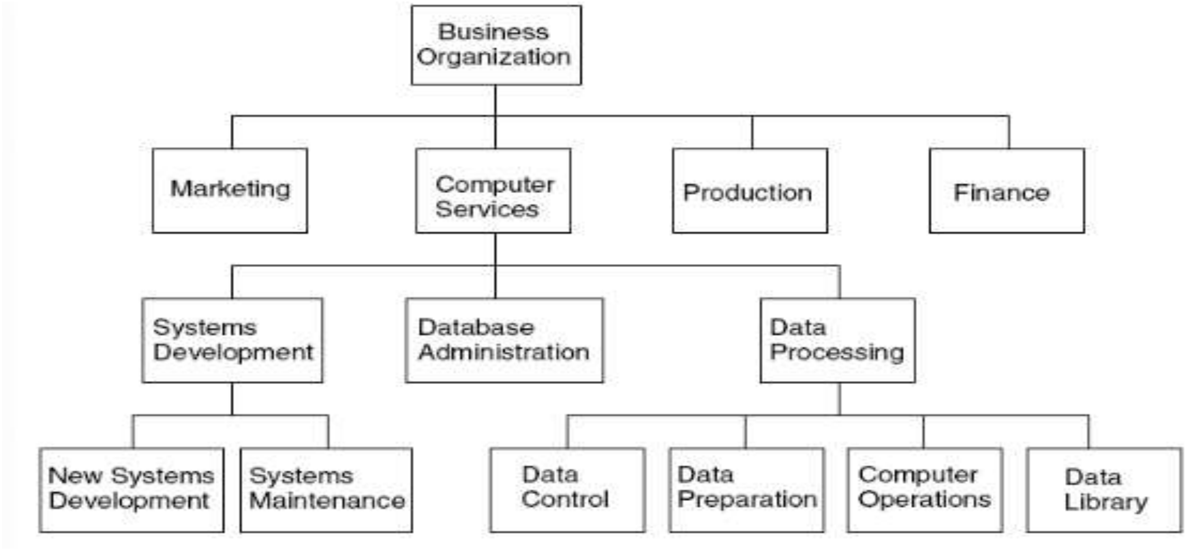
Distributed Data Processing
Most companies fall in between.
Centralized Data Processing

Reorganizing the computer services function into small information processing units that are distributed to end users and placed under their control

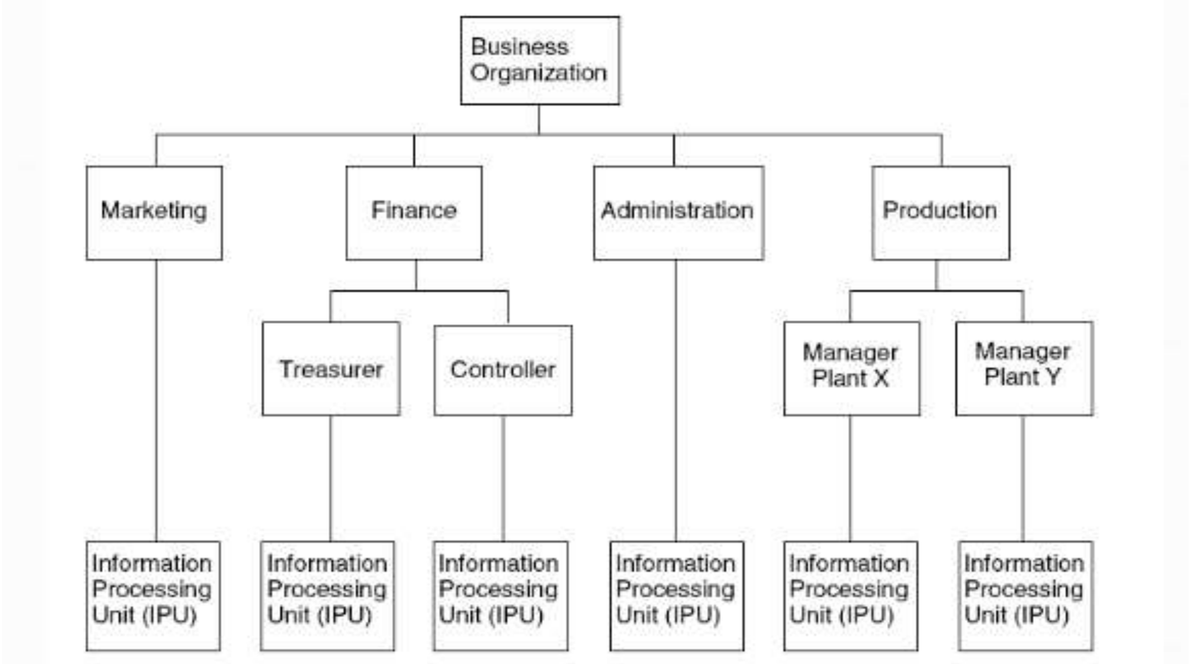
All data processing is performed by one or more large computers housed at a central site that serves users throughout the organization.

Primary areas:
database administration
data processing
systems development
systems maintenance

1.1.7.a Organization of Computer Services Function in a Centralized System



1.1.7.b Organizational Structure for a Distributed Processing System


Business Organization
Marketing
Finance
Administration
Production
Treasurer
Controller
Manager Plant X
Manager Plant Y
Information Processing Unit (IPU)
Information Processing Unit (IPU)
Information Processing Unit (IPU)
Information Processing Unit (IPU)
Information Processing Unit (IPU)
Information Processing Unit (IPU)

Potential Advantages of DDP

Cost reductions in hardware and data entry tasks. Improved cost control responsibility. Improved user satisfaction since control is closer to the user level. Backup of data can be improved through the use of multiple data storage sites.

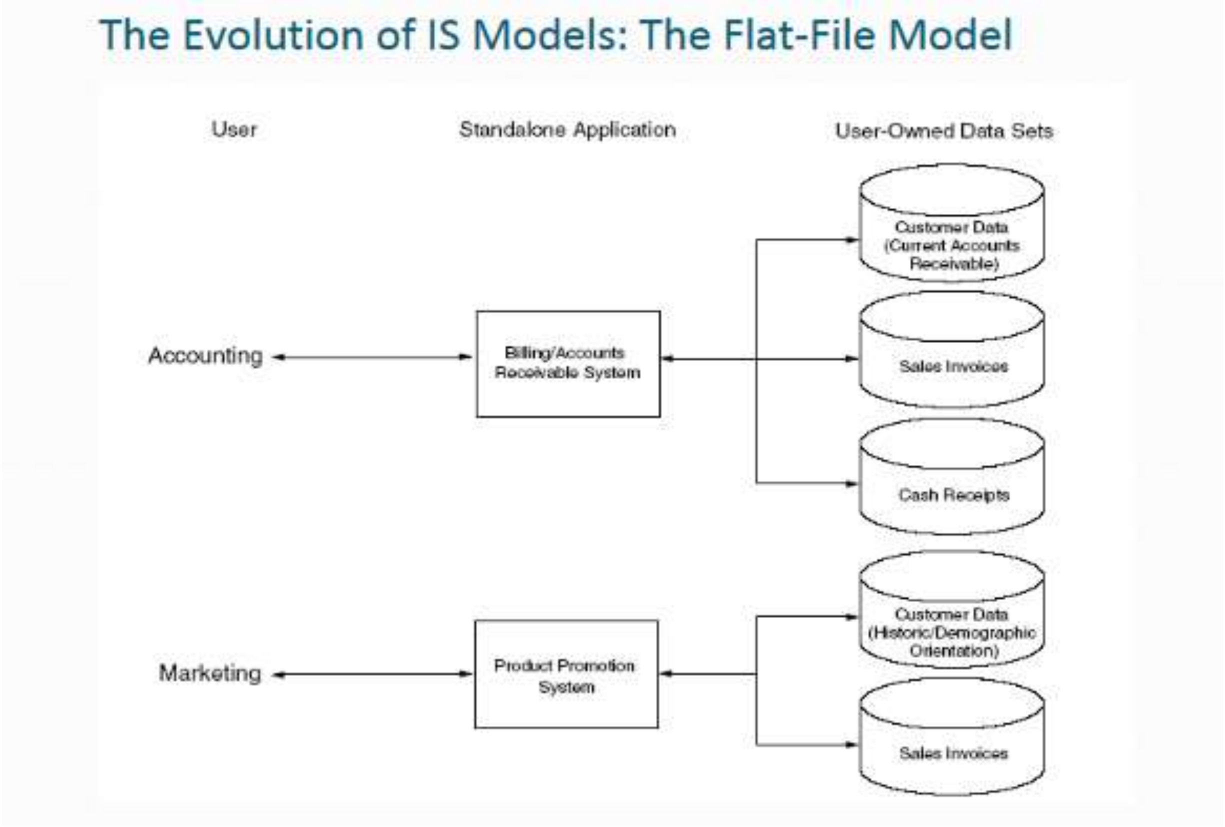
Potential Disadvantages of DDP

Loss of control, Mismanagement of company resources, Hardware and software incompatibility, Redundant tasks and data, Consolidating tasks usually segregated, Difficulty attracting qualified personnel and Lack of standards.

1.1.8 Manual Process Model

Transaction processing, information processing, and accounting are physically performed by people, usually using paper documents. Useful to study because: helps link AIS courses to other accounting courses, often easier to understand business processes when not shrouded in technology, facilitates understanding internal controls.

1.1.9 The evolution of IS Models: The Flat-File Model

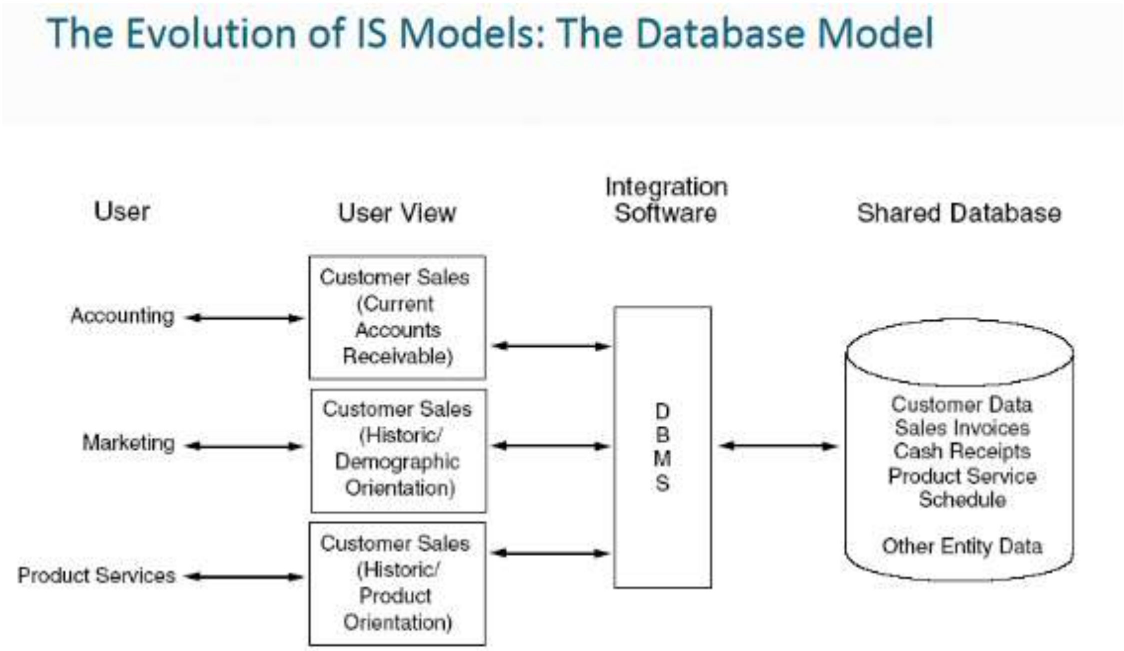


The Evolution of IS Models: The Flat-File Model

Data Redundancy Problems

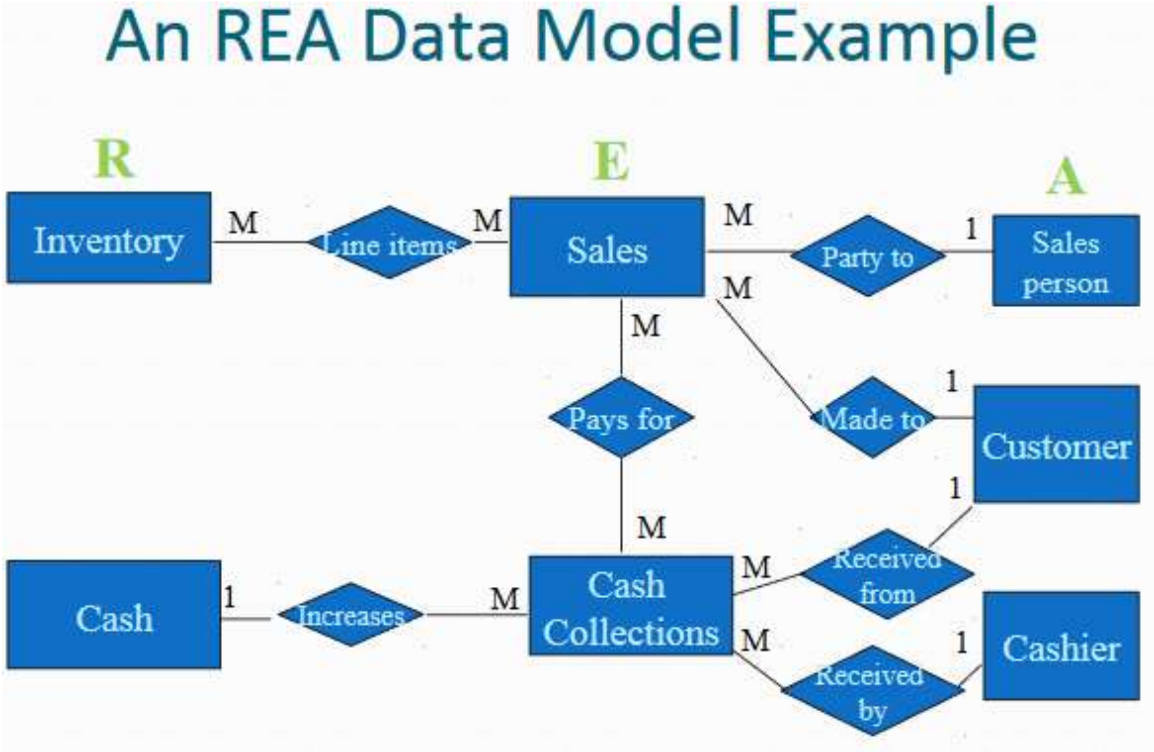
- **Data Storage** - excessive storage costs of paper documents and/or magnetic form.
- **Data Updating** - changes or additions must be performed multiple times.
- **Currency of Information -** potential problem of failing to update all affected files
- **Task-Data Dependency -** user’s inability to obtain additional information as needs change.
- **Data Integration -** separate files are difficult to integrate across multiple users

1.1.10 The Evolution of IS Models: The Database Model



The Evolution of IS Models: The Database Model

1.1.11 REA DATA MODEL EXAMPLE



An REA Data Model Example

1.1.12 REA Model (*shall be discussed more when designing an AIS in later units***)**

The REA model is an accounting framework for modeling an organization’s economic resources; e.g., assets, Economic events; i.e., affect changes in resources, economic agents; i.e., individuals and departments that participate in an economic event, Interrelationships among resources, events and agents.

Entity-relationship diagrams (ERD) are often used to model these relationships.

Accountants as Information System Users

Accountants must be able to clearly convey their needs to the systems professionals who design the system. The accountant should actively participate in systems development projects to ensure appropriate systems design.

1.1.13 Accountants as System Designers

The accounting function is responsible for the conceptual system, while the computer function is responsible for the physical system. The conceptual system determines the nature of the information required, its sources, its destination, and the accounting rules that must be applied.

Accountants as System Auditors

External Auditors - attest to fairness of financial statements, assurance service: broader in scope than traditional attestation audit.

IT Auditors - evaluate IT, often as part of external audit.

Internal Auditors - in-house IS and IT appraisal services

1.2 OVERVIEW OF BUSINESS PROCESS

Before going deep into what accounting information system is, its vital to under the business process and how it functions.

Objectively business process will bring out the following

- Basic business activities in which an organization engages
- Decisions to be made to undertake these activities
- The information required to make those decisions.
- The role that the data processing cycle play in organizing business activities and providing information to users.
- The role of the information system and enterprise resource planning in modern organizations.

What is a Business process? - Logically related sets of tasks or activities geared toward some business outcome. It can also be defined as a prescribed sequence of work steps performed in order to produce a desired result for the organization. A business process is initiated by a particular kind of event, has a well-defined beginning and end, and is usually completed in a relatively short period. Organizations have many different business processes, such as completing a sale, purchasing raw materials, paying employees, and paying vendors. Each business process has either a direct or an indirect effect on the financial status of the organization. For example, completing a sale directly increases cash or other assets, while paying employees directly reduces cash or increases liabilities. Purchasing new, efficient equipment also directly affects assets and/or liability accounts; yet this transaction is also expected to indirectly increase sales and assets, as it provides for increased productivity and an expanded customer base. Therefore, we can see why, as business processes occur, the accounting information system must capture and record the related accounting information. All of the possible business processes would be too numerous to list. However, the four general types of business processes typical in organizations (which will be described in later in this unit) are as follows

1. ***Revenue processes***;
   a. Sales processes
   b. Sales return processes
   c. Cash collection processes
2. ***Expenditure processes***
   a. Purchasing processes
   b. Purchase return processes
   c. Cash disbursement processes

d. Payroll processes
e. Fixed asset processes

3. Conversion processes

a. Planning processes
b. Resource management processes
c. Logistics processes

4. ***Administrative processes***

a. Capital processes
b. Investment processes
c. General ledger processes

1.2.1 INFORMATION NEEDS AND BUSINESS ACTIVITIES

Businesses engage in a variety of activities, including:

- Acquiring capital
- Buying buildings and equipment
- Hiring and training employees
- Purchasing inventory
- Doing advertising and marketing
- Selling goods or services
- Collecting payment from customers
- Paying employees
- Paying taxes
- Paying vendors

And each of these activities requires information to make these different types of decisions. Types of information needed for decision making may be financial or nonfinancial. The business or individual who make decisions may need information assistance from internal and external sources e.g (employee and management), customers, vendors, creditors, and governmental agencies as external respectively.

1.2.2 INTERACTION WITH EXTERNAL AND INTERNAL PARTIES

The interaction is typically two-way, in that the AIS sends information to and receives information from these parties.

A transaction is: – An agreement between two entities to exchange goods or services; *OR* – Any other event that can be measured in economic terms by an organization. EXAMPLES: Sell goods to customers. These transactions go round as long as the business is in continuity. Let us have a look at the meaning of business cycle and what it involves.

The transaction cycle is a process which begins with capturing data about a transaction and ends with an information output, such as financial statements. Many business activities are paired in give-get exchanges. The basic exchanges can be grouped into five major transaction cycles.

1. Revenue cycle,
2. Expenditure cycle,
3. Production cycle,
4. Human resources/payroll cycle,

5. Financing cycle

1. **REVENUE CYCLE.** The revenue cycle involves interactions with your customers. You sell goods or services and get cash. Other transactions in the revenue cycle include: Handle customer inquiries, Take customer orders, Approve credit sales, Check inventory availability, Initiate back orders, Pick and pack orders, Ship goods, Bill customers, Update sales and Accts Rec. for sales, Receive customer payments, Update Accts Rec. for collections, Handle sales returns, discounts, & bad debts, Prepare management reports, Send info to other cycles.

Note that the last activity in any cycle is to send information to other cycles.

2. **EXPENDITURE CYCLE**. The expenditure cycle involves interactions with your suppliers. You buy goods or services and pay cash.
3. **PRODUCTION CYCLE.** In the production cycle, raw materials and labor are transformed into finished goods. Give Raw Materials & Labor Get Finished Goods.
4. **HUMAN RESOURCES/ PAYROLL CYCLE**. The human resources cycle involves interactions with your employees. Employees are hired, trained, paid, evaluated, promoted, and terminated.
5. **FINANCING CYCLE.** The financing cycle involves interactions with investors and creditors. You raise capital (through stock or debt), repay the capital, and pay a return on it (interest or dividends).

In a BUSINESS CYCLES, Every transaction cycle, relates to other cycles. Interfaces with the general ledger and reporting system, which generates information for management and external parties. Let us take a few examples.

- General Ledger and Reporting System / Revenue Cycle Expenditure / Cycle Production Cycle Human Res./ Payroll Cycle Financing Cycle

  - ✓ The revenue cycle – Gets finished goods from the production cycle – Provides funds to the financing cycle – Provides data to the General Ledger and Reporting System Finished Goods.

General Ledger and Reporting System Revenue Cycle, Expenditure Cycle Production Cycle Human Res./ Payroll Cycle Financing Cycle.

The expenditure cycle – Gets funds from the financing cycle – Provides raw materials to the production cycle – Provides data to the General Ledger and Reporting System Raw Mats.

The production cycle: – Gets raw materials from the expenditure cycle, Gets labor from the HR/payroll cycle, Provides finished goods to the revenue cycle, Provides data to the General Ledger and Reporting System Raw Mats. Finished Goods
The HR/payroll cycle: Gets funds from the financing cycle, Provides labor to the production cycle – Provides data to the General Ledger and Reporting System Funds.
The Financing cycle: – Gets funds from the revenue cycle, Provides funds to the expenditure and HR/payroll cycles, in return, Provides data to the General Ledger and Reporting System Funds.
The General Ledger and Reporting System: – Gets data from all of the cycles, Provides information for internal and external users Data.

Many accounting software packages implement different transaction cycles as separate modules. Not every module is needed in every organization, e.g., retail companies don't have a production cycle. Some companies may need extra modules. The implementation of each transaction cycle can differ significantly across companies. However the cycles are implemented, it is critical that the AIS be able to: Accommodate the information needs of managers, Integrate financial and nonfinancial data.

1.2.3 THE DATA PROCESSING CYCLE. Accountants play an important role in data processing. They answer questions such as:

- ❖ What data should be entered and stored?,
- ❖ Who should be able to access the data?
- ❖ How should the data be organized, updated, stored, accessed, and retrieved?
- ❖ How can scheduled and unanticipated information needs be met.
- ❖ To answer these questions, they must understand data processing concepts.

An important function of the AIS is to efficiently and effectively process the data about a company's transactions. In manual systems, data is entered into paper journals and ledgers. While in computer-based systems, the series of operations performed on data is referred to as the data processing cycle. The data processing cycle consists of four steps:

- Data input
- Data storage
- Data processing
- Information output

The first step in data processing is to capture the data. Usually triggered by a business activity. Data is captured about: – The event that occurred – The resources affected by the event – The agents who participated. These shall be discussed later in detail

DATA INPUT- A number of actions can be taken to improve the accuracy and efficiency of data input: Turnaround documents

- Source data automation
- Capture data with minimal human intervention. **Examples:** – ATMs for banking – Point-of-sale (POS) scanners in retail stores – Automated gas pumps that accept your credit card. Turnaround documents. ***Example:*** The stub on your telephone bill that you tear off and return with your check when you pay the bill. The customer account number is coded on the document, usually in machine-readable form, which reduces the probability of human error in applying the check to the correct account. Other actions that can be taken to improve the accuracy and efficiency of data input:

What does it mean if there are duplicate document numbers? – Using pre-numbered documents or having the system automatically assign sequential numbers to transactions. A number of actions can be taken to improve the accuracy and efficiency of data input: – Turnaround documents – Source data automation – Well-designed source documents and data entry screens – Using pre-numbered documents or having the system automatically assign sequential numbers to transactions – Verify • transactions **Example**: Check for inventory availability before completing an online sales transaction.

DATA STORAGE. Data needs to be organized for easy and efficient access. Vocabulary terms with respect to data storage.

i. ***Ledger DATA STORAGE.*** A ledger is a file used to store cumulative information about resources and agents. We typically use the word ledger to describe the set of t-accounts. The t-account is where we keep track of the beginning balance, increases, decreases, and ending balance for each asset, liability, owners' equity, revenue, expense, gain, loss, and dividend account.

- ***General ledger.*** The general ledger is the summary level information for all accounts. Detail information is not kept in this account.

- **Subsidiary ledger**. The subsidiary ledgers contain the detail accounts associated with the related general ledger account.
- ***Coding techniques.*** Coding is a method of systematically assigning numbers or letters to data items to help classify and organize them. There are many types of codes including: – Sequence codes – Block codes – Group codes 10/18/2014 58

In manual systems and some accounting packages, the first place that transactions are entered is the journal. – A general journal is used to record: Non-routine transactions, such as loan payments • Summaries of routine transactions • Adjusting entries • Closing entries • Ledger • General ledger • Subsidiary ledger • Coding techniques • Chart of accounts • Journals – A special journal is used to record routine transactions. The most common special journals are: • Cash receipts • Cash disbursements • Credit sales • Credit purchases.

Now that we've learned some storage terminology, let's return to the data storage process. • When transaction data is captured on a source document, the next step is to record the data in a journal. A journal entry is made for each transaction showing the accounts and amounts to be credited.

Now let's moving on to discussing some computer-based storage concepts, including: – Entity, Attribute, Record, Data Value, Field, File, Master File, Transaction File, and Database.

i. An entity is something about which information is stored. In your university's student information system, one entity is the student. The student information system stores information about students. What are some other entities in your student information system?

ii. Attributes are characteristics of interest with respect to the entity. Some attributes that a student information system typically stores about the student entity are: – Student ID number – Phone number – Address. What are some other attributes about students that a university might store?

iii. A field is the physical space where an attribute is stored. The space where the student ID number is stored is the student ID field. Col. 1-9 Col. 10-30 Col. 31-40 Col. 41-50 328469993 SIMPSON ALICE 4053721111 328500732 ANDREWS BARRY 4057440236 529036409 FLANDERS CARLA 4057475863

iv. A record is the set of attributes stored for a particular instance of an entity. The combination of attributes stored for Barry Andrews is Barry's record. Col. 1-9 Col. 10-30 Col. 31-40 Col. 41-50 328469993 SIMPSON ALICE 4053721111 328500732 ANDREWS BARRY 4057440236 529036409 FLANDERS CARLA 4057475863.

v. A data value is the intersection of the row and column. The data value for Barry Andrews' phone number is 405-744-0236. Col. 1-9 Col. 10-30 Col. 31-40 Col. 41-50 328469993 SIMPSON ALICE 4053721111 328500732 ANDREWS BARRY 4057440236 529036409 FLANDERS CARLA 4057475863

vi. A file is a group of related records. The collection of records about all students at the university might be called the student file. If there were only three students and four attributes stored for each student, the file might appear as shown below: Col. 1-9 Col. 10-30 Col. 31-40 Col. 41-50

328469993 SIMPSON ALICE 4053721111 328500732 ANDREWS BARRY 4057440236 529036409 FLANDERS CARLA 4057475863.

vii. A master file is a file that stores cumulative information about an organization's entities. It is conceptually similar to a ledger in a manual AIS in that: – The file is permanent – The file exists across fiscal periods – Changes are made to the file to reflect the effects of new transactions.

viii. A transaction file is a file that contains records of individual transactions (events) that occur during a fiscal period. It is conceptually similar to a journal in a manual AIS in that: – The files are temporary – The files are usually maintained for one fiscal period

ix. A database is a set of interrelated, centrally-coordinated files. When files about students are integrated with files about classes and files about instructors, we have a database. Student File Class File Instructor File.

1.2.4 THE DATA PROCESSING CYCLE

The data processing cycle consists of four steps: – Data input – Data storage – Data processing – Information output. Once data about a business activity has been collected and entered into a system, it must be processed. There are four different types of file processing: – Updating data to record the occurrence of an event, the resources affected by the event, and the agents who participated, e.g., recording a sale to a customer. – Changing data, e.g., a customer address – Adding data, e.g., a new customer. – DELETING DATA, E.G., REMOVING AN OLD CUSTOMER THAT HAS NOT PURCHASED ANYTHING IN 5 YEARS.

INFORMATION OUTPUT. The final step in the information process is information output. This output can be in the form of:

x. ***Documents.*** Documents are records of transactions or other company data. *EXAMPLE*: Employee paychecks or purchase orders for merchandise, Documents generated at the end of the transaction processing activities are known as operational documents (as opposed to source documents). They can be printed or stored as electronic images.

xi. ***Reports***. Reports are used by employees to control operational activities and by managers to make decisions and design strategies. They may be produced: – On a regular basis – On an exception basis – On demand • Organizations should periodically reassess whether each report is needed.

xii. ***Queries***. Queries are user requests for specific pieces of information. They may be requested: – Periodically – One time • They can be displayed: – On the monitor, called soft copy – On the screen, called hard copy

Output can serve a variety of purposes: – Financial statements can be provided to both external and internal parties. – Some outputs are specifically for internal use: For planning purposes. ***Examples*** of outputs for planning purposes include:

- ➢ Budgets • Budgets are an entity's formal expression of goals in financial terms – Sales forecasts.
- ➢ Performance reports are outputs that are used for control purposes. Output can serve a variety of purposes: These reports compare an organization's standard or expected performance with its actual outcomes. Management by exception is an approach to utilizing performance reports that focuses

on investigating and acting on only those variances that are significant. For planning purposes, for management of day-to-day operations and for control purposes.

The traditional AIS captures financial data. These data may be financial and Non-financial data.

Enterprise resource planning (ERP) systems are designed to integrate all aspects of a company’s operations (including both financial and non-financial information) with the traditional functions of an AIS.

SUMMARY

• We’ve learned about the basic business activities in which an organization engages, the decisions that need to be made, and the information required to make those decisions.

• We’ve reviewed the data processing cycle and its role in organizing business activities and providing information to users.

• Finally, we’ve touched on the role of the information systems in modern organizations and introduced the notion of enterprise resource planning systems.

UNIT 2

2.0 RELATIONAL DATA BASES, SYSTEM DEVELOPMENT AND DOCUMENTATION TECHNIQUES.

Study objective questions

- How are databases different than file-based legacy systems?
- Why are databases important and what is their advantage?
- What is the difference between logical and physical views of a database?
- What are the fundamental concepts of database systems such as DBMS, schemas, the data dictionary, and DBMS languages?
- What is a relational database, and how does it organize data?
- How are tables structured to properly store data in a relational database?

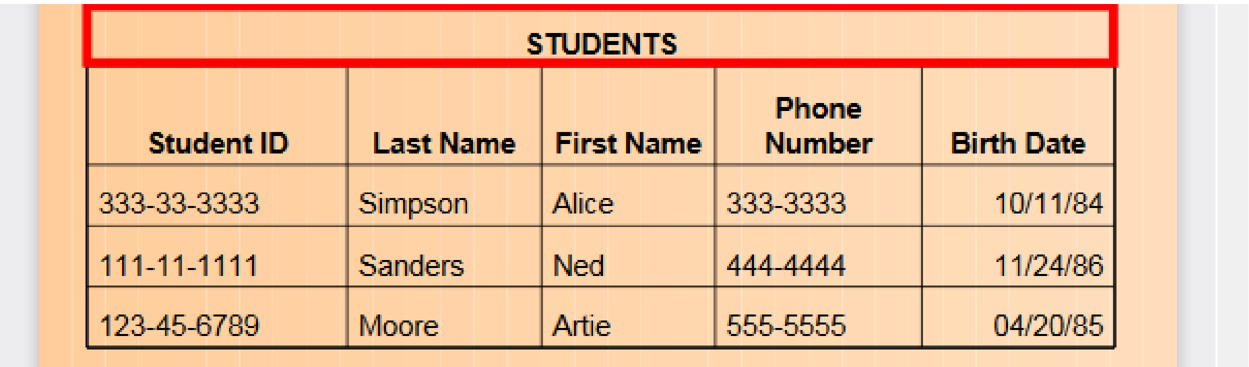
2.1 Introduction

Relational databases underlie most modern integrated AISs. They are the most popular type of database used for transaction processing. In this chapter, we’ll define the concept of a database.

FILE VS. DATABASES

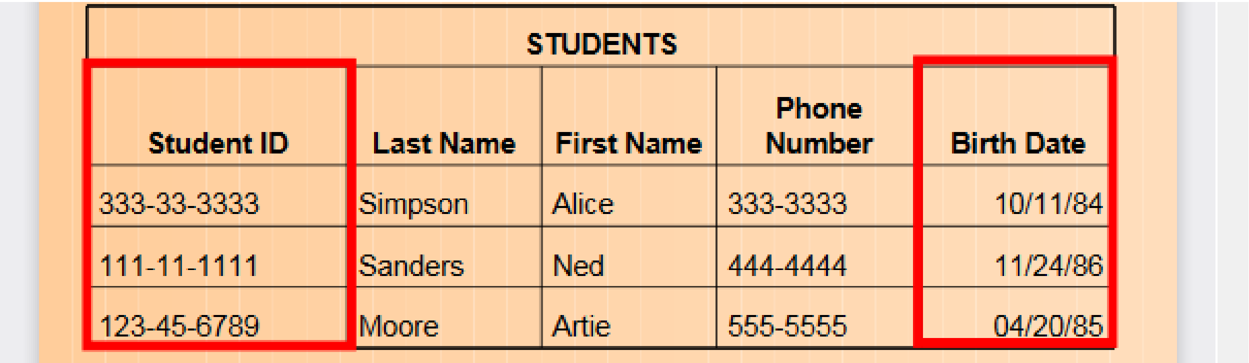
Let’s examine some basic principles about how data are stored in computer systems.

An entity is anything about which the organization wishes to store data. At your college or university, one entity would be the student.



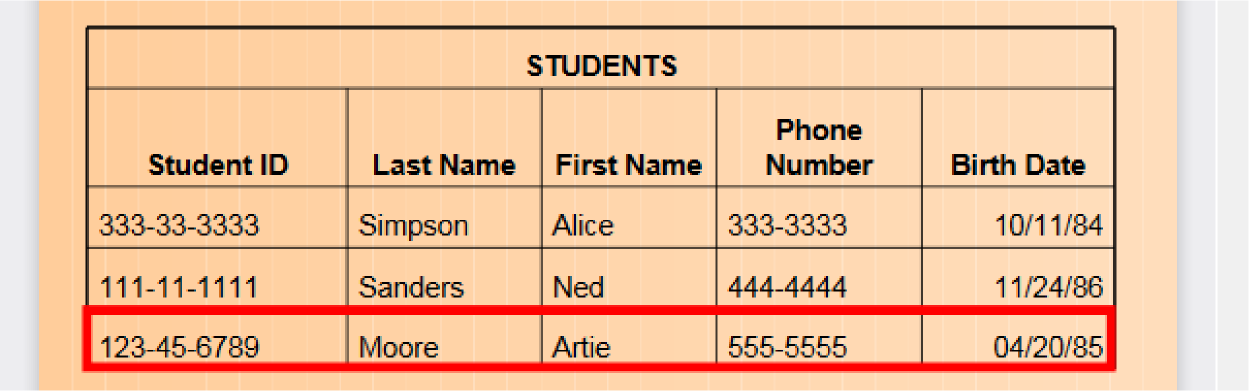
STUDENTS				
Student ID	Last Name	First Name	Phone Number	Birth Date
333-33-3333	Simpson	Alice	333-3333	10/11/84
111-11-1111	Sanders	Ned	444-4444	11/24/86
123-45-6789	Moore	Artie	555-5555	04/20/85

Information about the ***attributes*** of an entity (e.g., the student's ID number and birth date) are stored in ***fields.***



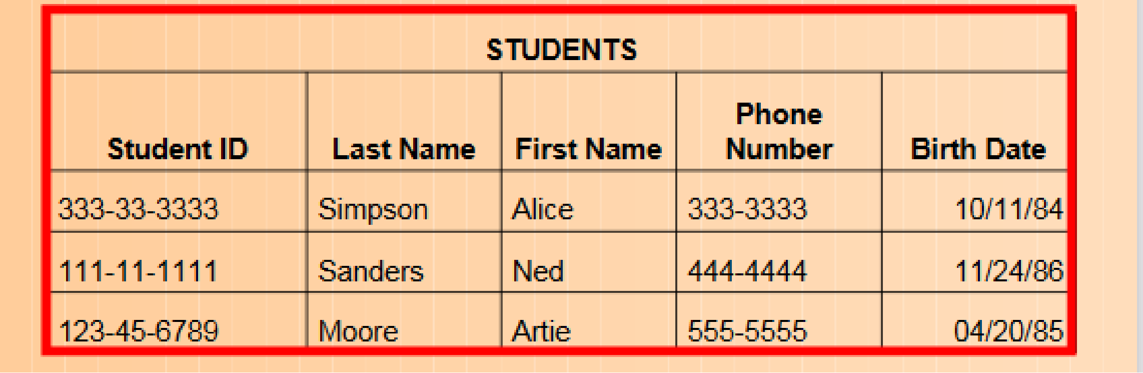
STUDENTS				
Student ID	Last Name	First Name	Phone Number	Birth Date
333-33-3333	Simpson	Alice	333-3333	10/11/84
111-11-1111	Sanders	Ned	444-4444	11/24/86
123-45-6789	Moore	Artie	555-5555	04/20/85

All the fields containing data about one entity (e.g., one student) form a record.–The example below shows the record for Artie Moore



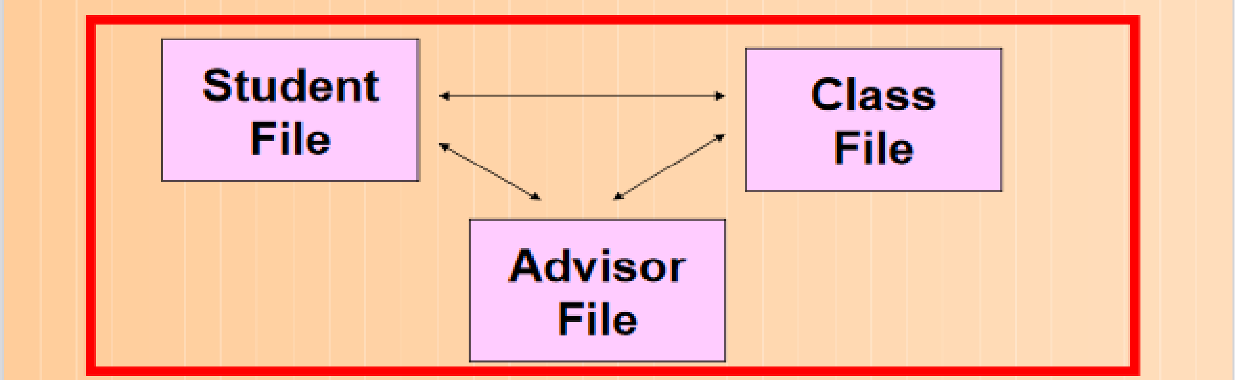
STUDENTS				
Student ID	Last Name	First Name	Phone Number	Birth Date
333-33-3333	Simpson	Alice	333-3333	10/11/84
111-11-1111	Sanders	Ned	444-4444	11/24/86
123-45-6789	Moore	Artie	555-5555	04/20/85

A set of all related records forms a file (e.g., the student file).–If this university only had three students and five fields for each student, then the entire file would be depicted below.

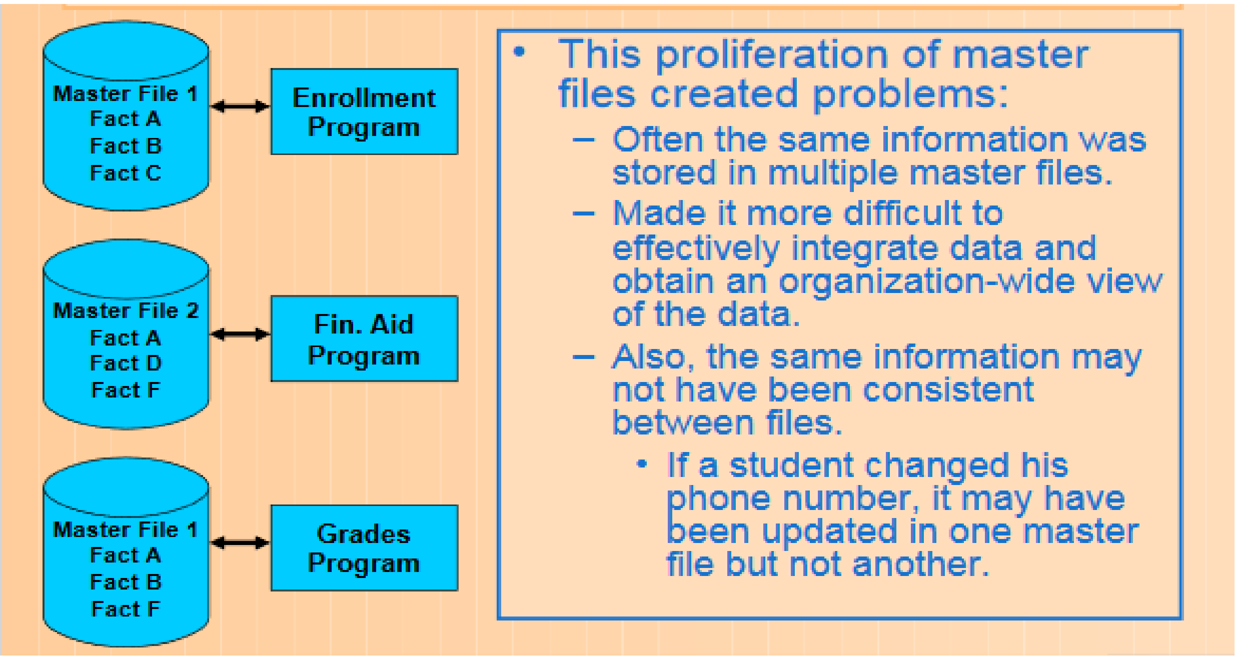


STUDENTS				
Student ID	Last Name	First Name	Phone Number	Birth Date
333-33-3333	Simpson	Alice	333-3333	10/11/84
111-11-1111	Sanders	Ned	444-4444	11/24/86
123-45-6789	Moore	Artie	555-5555	04/20/85

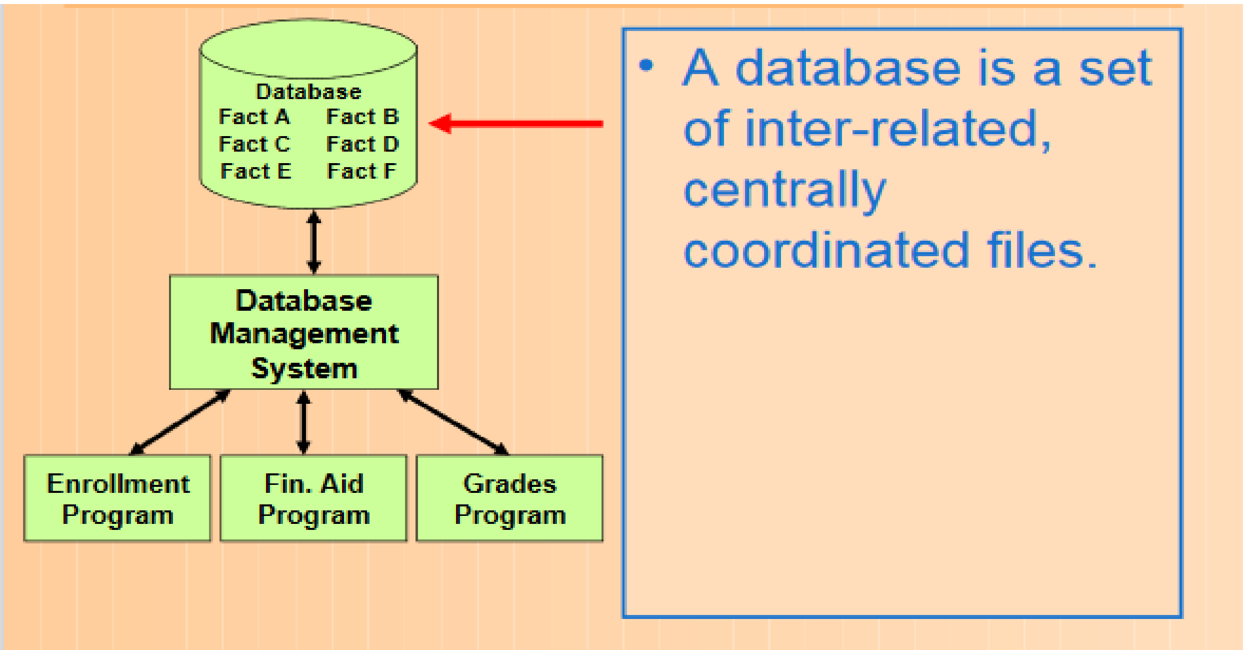
A set of interrelated, centrally coordinated files forms a *database.*



Database systems were developed to address the problems associated with the proliferation of master files. For years, each time a new information need arose, companies created new files and programs. The result was a significant increase in the number of master files.

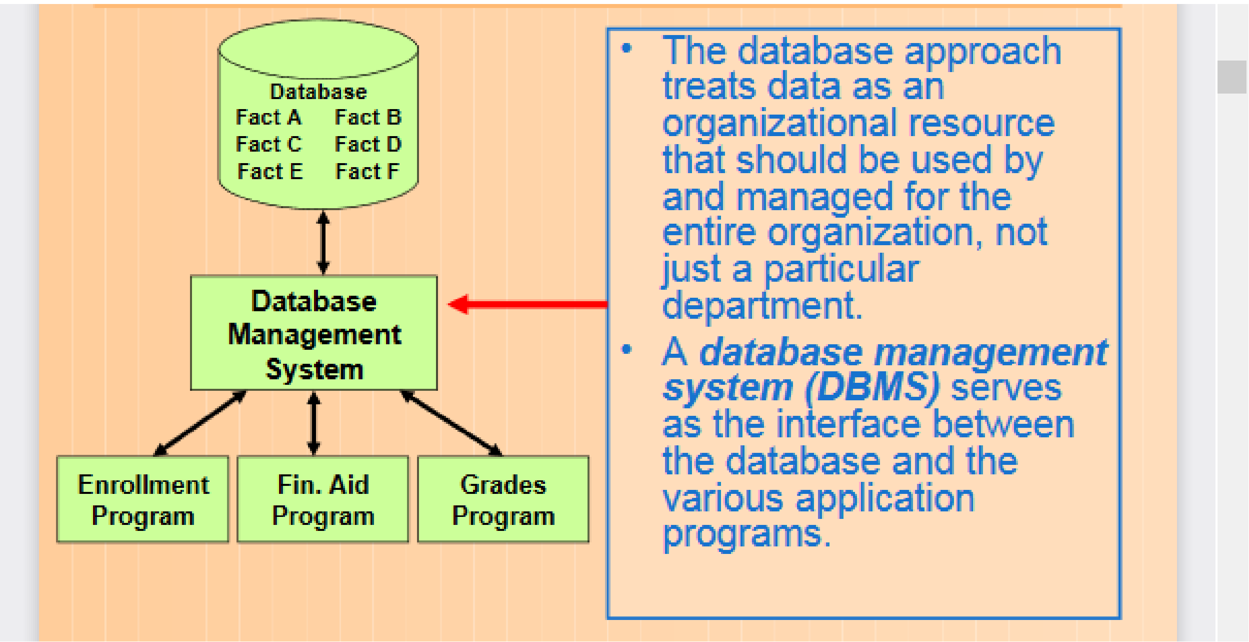


- This proliferation of master files created problems:
  - Often the same information was stored in multiple master files.
  - Made it more difficult to effectively integrate data and obtain an organization-wide view of the data.
  - Also, the same information may not have been consistent between files.
    - If a student changed his phone number, it may have been updated in one master file but not another.

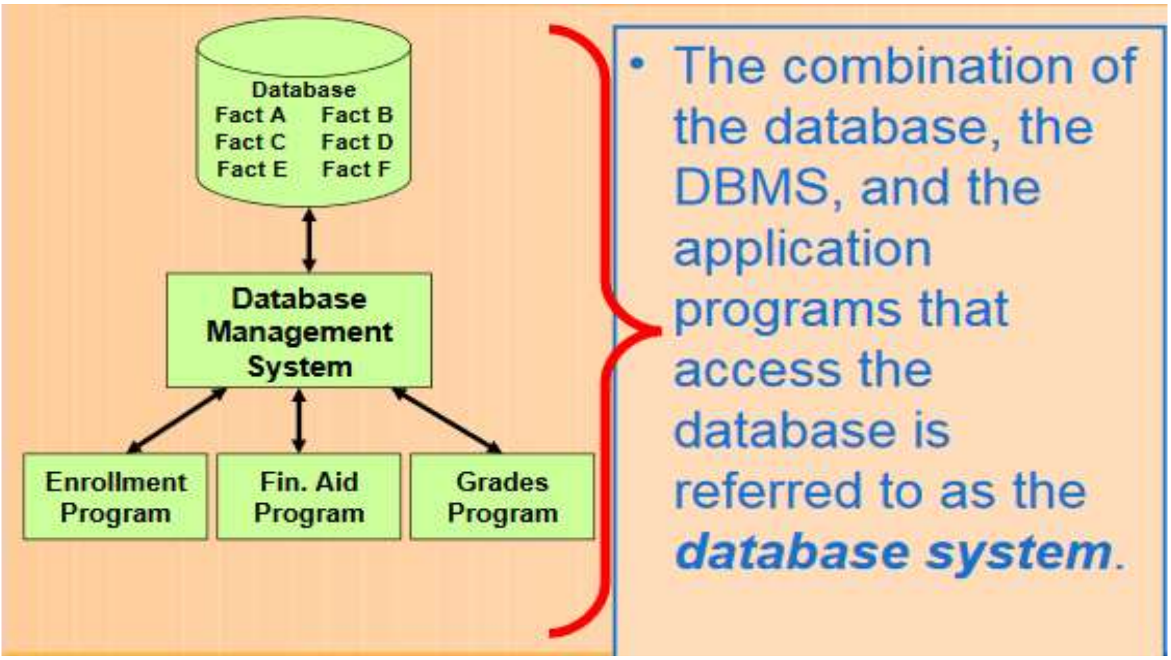


- A database is a set of inter-related, centrally coordinated files.

The database approach treats data as an organizational resource that should be used by and managed for the entire organization, not just a particular department. ***A database management system (DBMS)*** serves as the interface between the database and the various application programs



- The database approach treats data as an organizational resource that should be used by and managed for the entire organization, not just a particular department.
- A ***database management system (DBMS)*** serves as the interface between the database and the various application programs.



Database
Fact A Fact B
Fact C Fact D
Fact E Fact F

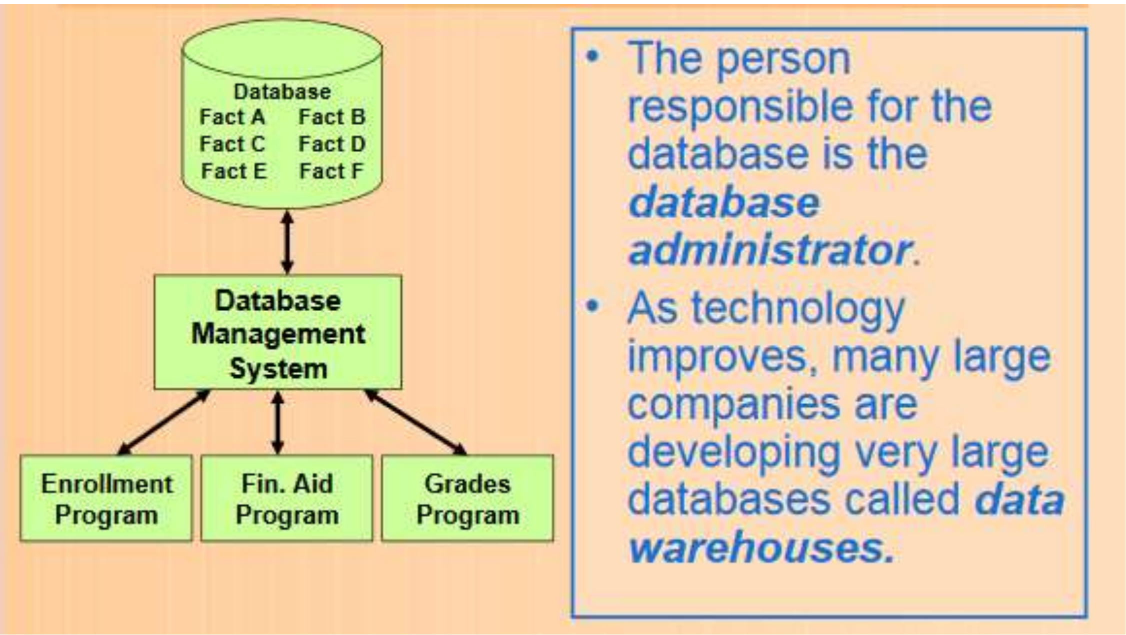
Database Management System

Enrollment Program

Fin. Aid Program

Grades Program

- The combination of the database, the DBMS, and the application programs that access the database is referred to as the ***database system***.



Database
Fact A Fact B
Fact C Fact D
Fact E Fact F

Database Management System

Enrollment Program

Fin. Aid Program

Grades Program

- The person responsible for the database is the ***database administrator***.
- As technology improves, many large companies are developing very large databases called ***data warehouses.***

IMPORTANCE AND ADVANTAGES OF DATABASE SYSTEMS

1. Database technology is everywhere. Most new AISs implement a database approach. Virtually all mainframe computer sites use database technology. Use of databases with PCs is growing also.
2. As accountants, you are likely to audit or work for companies that use database technology to store, process, and report accounting transactions. Many accountants work directly with databases and will enter, process, and query databases. Some will develop and evaluate internal controls necessary to ensure database integrity. Others will be involved in the design and management of databases

Database technology provides the following benefits to organizations:

i. *Data integration* - Achieved by combining master files into larger pools of data accessible by many programs.

ii. *Data sharing* - It's easier to share data that's integrated.

iii. *Reporting flexibility* - Reports can be revised easily and generated as needed. The database can easily be browsed to research problems or obtain detailed information.

iv. *Minimal data redundancy and inconsistencies* - Because data items are usually stored only once.

v. *Data independence* - Data items are independent of the programs that use them. Consequently, a data item can be changed without changing the program and vice versa. Makes programming easier and simplifies data management.

vi. *Central management of data* - Data management is more efficient because the database administrator is responsible for coordinating, controlling, and managing data.

vii. *Cross-functional analysis* - Relationships can be explicitly defined and used in the preparation of management reports. Example: Relationship between selling costs and promotional campaigns.

2.2 DATABASE SYSTEMS

Logical and Physical Views of Data

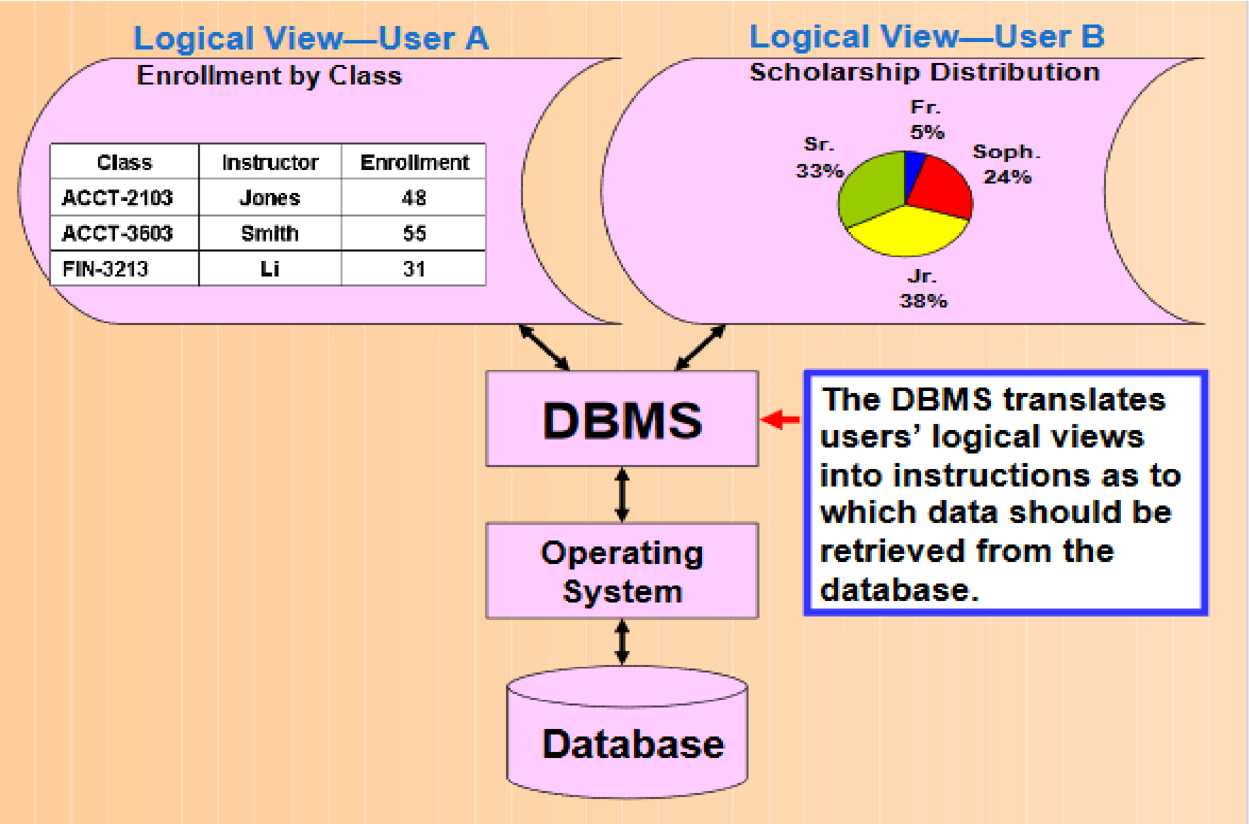
In file-oriented systems, programmers must know the physical location and layout of records used by a program. They must reference the location, length, and format of every field they utilize. When data is used from several files, this process becomes more complex.

Database systems overcome this problem by separating the storage and use of data elements. Two separate views of the data are provided:

i. Logical view - How the user or programmer conceptually organizes and understands the data.

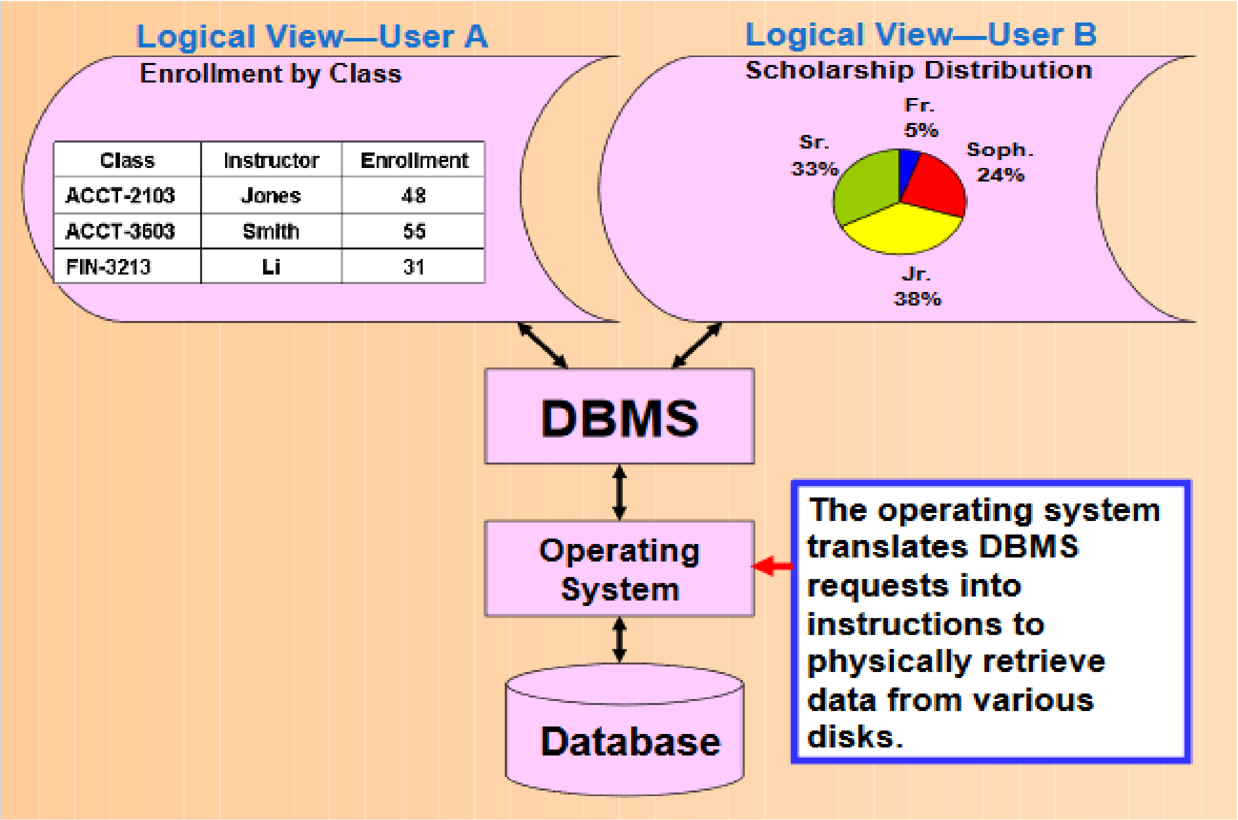
ii. Physical view - How and where the data are physically arranged and stored.

Separating these views facilitates application development, because programmers can focus on coding the logic and not be concerned with storage details.



Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3603	Smith	55
FIN-3213	Li	31

The DBMS translates users' logical views into instructions as to which data should be retrieved from the database.



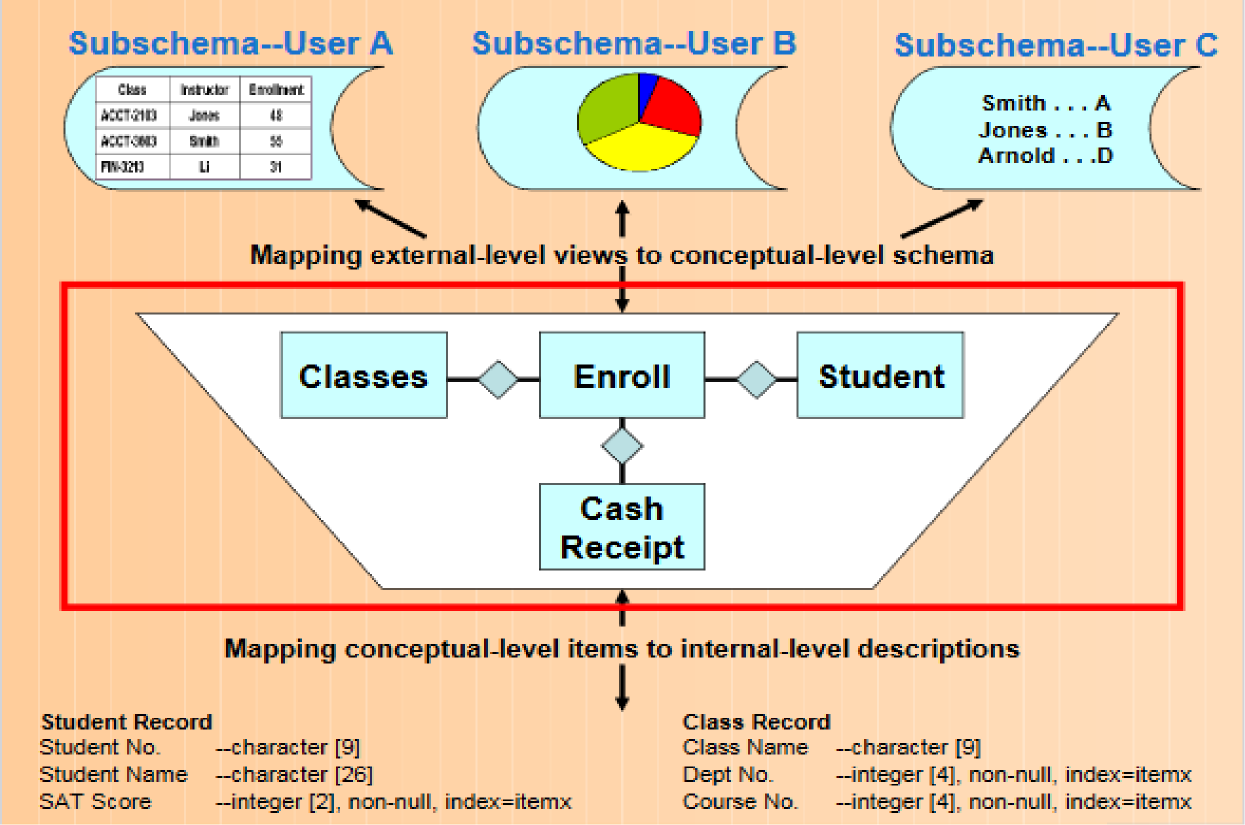
Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3603	Smith	55
FIN-3213	Li	31

The operating system translates DBMS requests into instructions to physically retrieve data from various disks.

The DBMS handles the link between the physical and logical views of the data. Allows the user to access, query, and update data without reference to how or where it is physically stored. The user only needs to define the logical data requirements. Separating the logical and physical views of data also means users can change their conceptualizations of the data relationships without making changes in the physical storage. The database administrator can also change the physical storage of the data without affecting users or application programs.

Schemas – A schema describes the logical structure of a database. There are three levels of schema.

i. Conceptual level - The organization-wide view of the *entire* database — i.e., the big picture. Lists all data elements and the relationships between them.

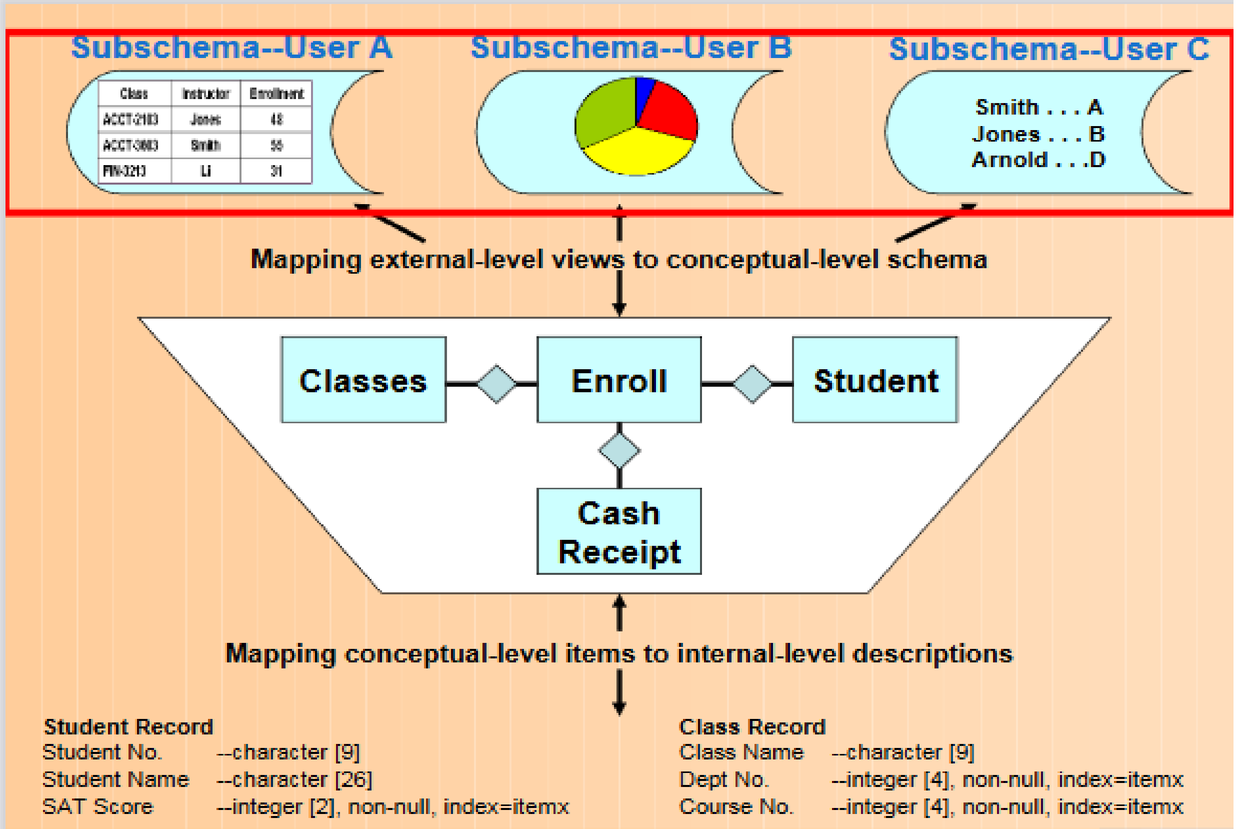


Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3603	Smith	55
FIN-3213	Li	31

Student Record	
Student No.	--character [9]
Student Name	--character [26]
SAT Score	--integer [2], non-null, index=itemx

Class Record	
Class Name	--character [9]
Dept No.	--integer [4], non-null, index=itemx
Course No.	--integer [4], non-null, index=itemx

ii. **External level** - A set of individual user views of portions of the database, i.e., how each user sees the portion of the system with which he interacts. These individual views are referred to as subschema.



Subschema--User A

Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3603	Smith	55
FIN-3213	Li	31

Subschema--User B

Subschema--User C

Smith . . . A
Jones . . . B
Arnold . . .D

Mapping external-level views to conceptual-level schema

Mapping conceptual-level items to internal-level descriptions

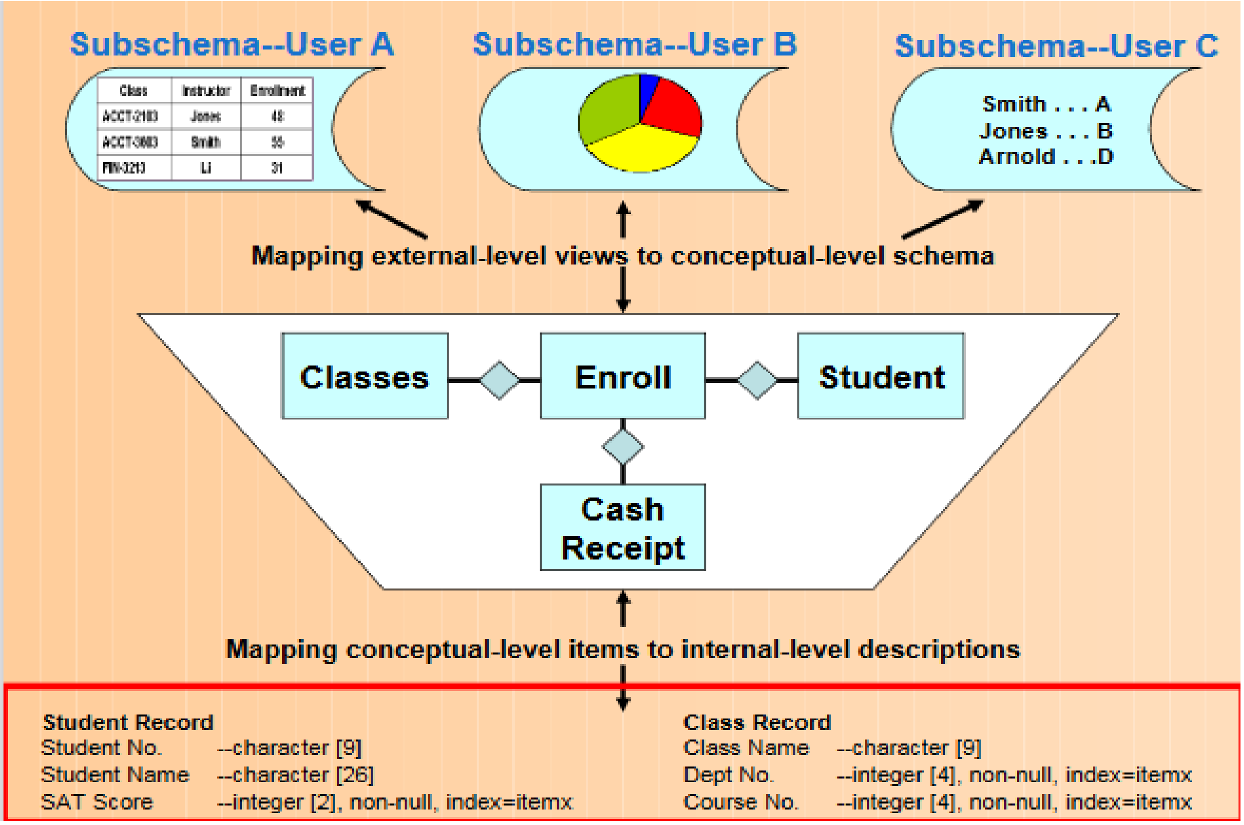
Student Record

Student No.	--character [9]
Student Name	--character [26]
SAT Score	--integer [2], non-null, index=itemx

Class Record

Class Name	--character [9]
Dept No.	--integer [4], non-null, index=itemx
Course No.	--integer [4], non-null, index=itemx

iii. Internal level - A low-level view of the database. It describes how the data are actually stored and accessed including: Record layouts, Definitions, Addresses and Indexes.



Subschema--User A

Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3803	Smith	55
FIN-3213	Li	31

Subschema--User B

Subschema--User C

Smith . . . A
Jones . . . B
Arnold . . .D

Mapping external-level views to conceptual-level schema

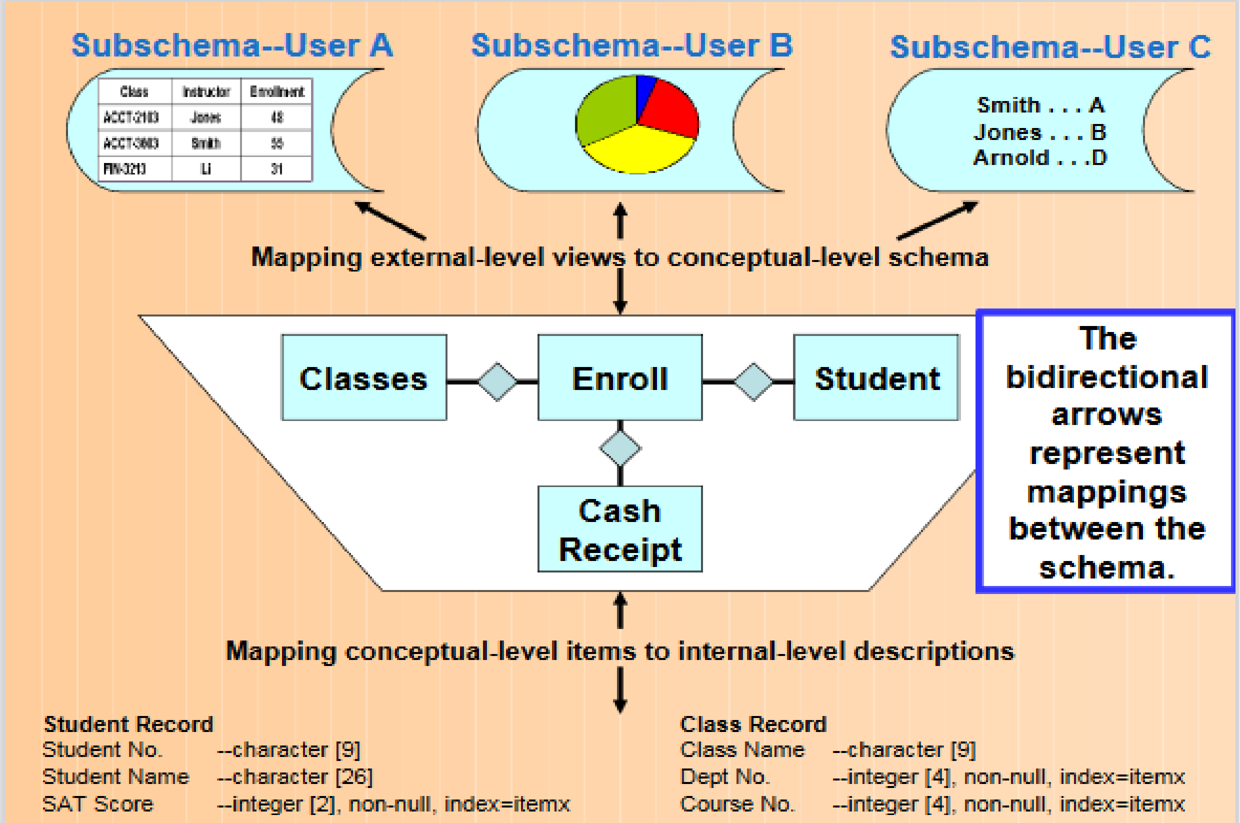
Mapping conceptual-level items to internal-level descriptions

Student Record

Student No.	--character [9]
Student Name	--character [26]
SAT Score	--integer [2], non-null, index=itemx

Class Record

Class Name	--character [9]
Dept No.	--integer [4], non-null, index=itemx
Course No.	--integer [4], non-null, index=itemx



Subschema--User A

Class	Instructor	Enrollment
ACCT-2103	Jones	48
ACCT-3803	Smith	55
FIN-3213	Li	31

Subschema--User B

Subschema--User C

Smith . . . A
Jones . . . B
Arnold . . .D

Mapping external-level views to conceptual-level schema

The bidirectional arrows represent mappings between the schema.

Mapping conceptual-level items to internal-level descriptions

Student Record

Student No.	--character [9]
Student Name	--character [26]
SAT Score	--integer [2], non-null, index=itemx

Class Record

Class Name	--character [9]
Dept No.	--integer [4], non-null, index=itemx
Course No.	--integer [4], non-null, index=itemx

The DBMS uses the mappings to translate a request by a user or program for data (expressed in logical names and relationships) into the indexes and addresses needed to physically access the data. Accountants are frequently involved in developing conceptual - and external - level schema. An employee's access to data should be limited to the subschema of data that is relevant to the performance of his job.

2.2.1 The Data Dictionary – A key component of a DBMS is the data dictionary. Contains information about the structure of the database. For each data element, there is a corresponding record in the data dictionary describing that element.

Information provided for each element includes: A description or explanation of the element. The records in which it is contained. Its source. The length and type of the field in which it is stored. The programs in which it is used. The outputs in which it is contained. The authorized users of the element. Other names for the element.

Accountants should participate in the development of the data dictionary because they have a good understanding of the data elements in a business organization, as well as where those elements originate and how they are used.

The DBMS usually maintains the data dictionary.–It is often one of the first applications of a newly implemented database system.

Inputs to the dictionary include:

i. Records of new or deleted data elements.

ii. Changes in names, descriptions, or uses of existing elements.

Outputs include:

Reports that are useful to programmers, database designers, and IS users in:

i. Designing and implementing the system.

ii. Documenting the system.

iii. Creating an audit trail.

2.2.2 DBMS Languages

Every DBMS must provide a means of performing the three basic functions of:

1. Creating a database
2. Changing a database
3. Querying a database

i. **Creating a database**: The set of commands used to create the database is known as *data definition* language (DDL). DDL is used to:

a. Build the data dictionary

b. Initialize or create the database

c. Describe the logical views for each individual user or programmer

d. Specify any limitations or constraints on security imposed on database records or fields

ii. **Changing a database:** The set of commands used to change the database is known as ***data manipulation language*** (DML). DML is used for maintaining the data including: Updating data, Inserting data, Deleting portions of the database

iii. Querying a database: The set of commands used to query the database is known ***as data query language*** (DQL). DQL is used to interrogate the database, including: Retrieving records, Sorting records, Ordering records, Presenting subsets of the database.

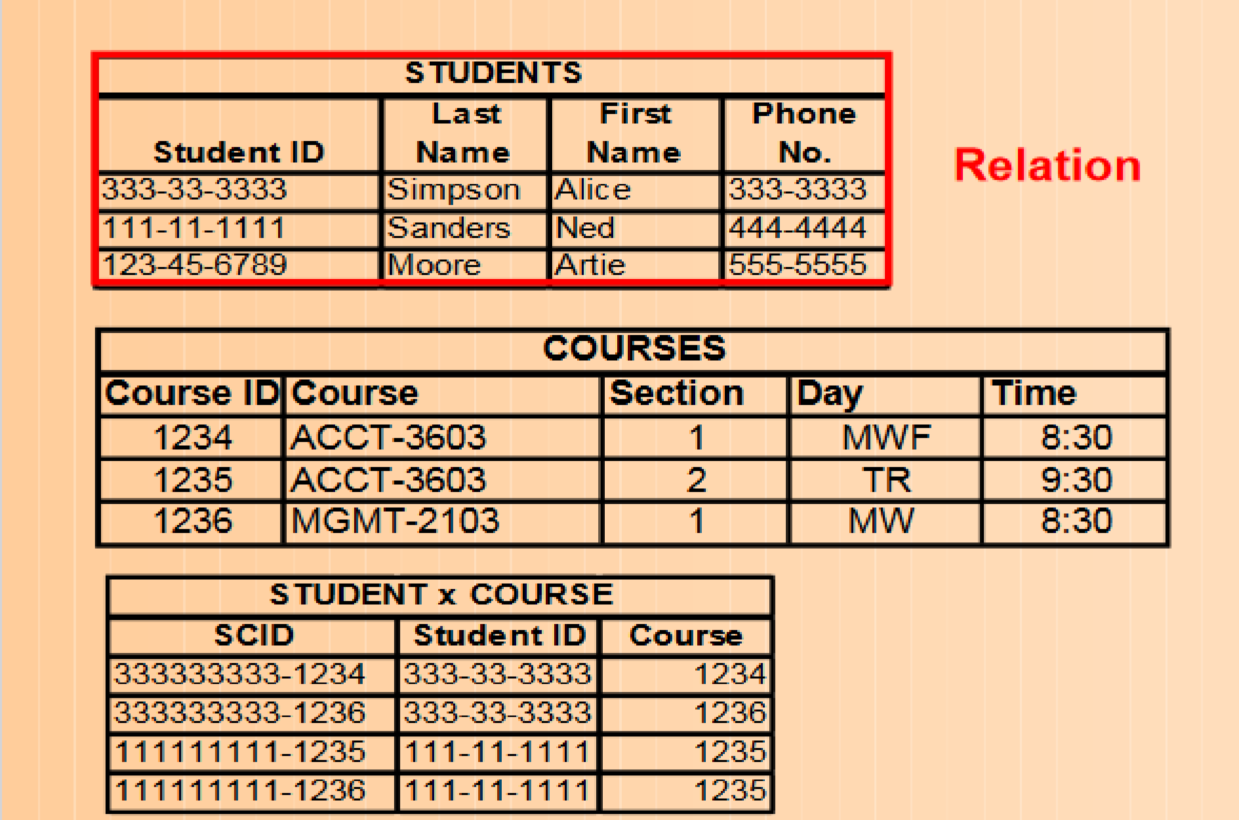
The DQL usually contains easy-to-use, powerful commands that enable users to satisfy their own information needs.

2.2.3 Report Writer

Many DBMS packages also include a report writer, a language that simplifies the creation of reports. Users typically specify: *What elements they want printed, and how the report should be formatted.*

The report writer then: Searches the database, Extracts specified data, Prints them out according to specified format. Users typically have access to both DQL and report writer. Access to DQL and DML are typically restricted to employees with administrative and programming responsibilities.

A DBMS is characterized by the type of logical data model on which it is based. A *Data Model* is an abstract representation of the contents of a database. Most new DBMSs are called relational databases because they use the relational model developed by E.F. Codd in 1970. The relational data model represents everything in the database as being stored in the forms of tables (aka, relations).



STUDENTS

Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

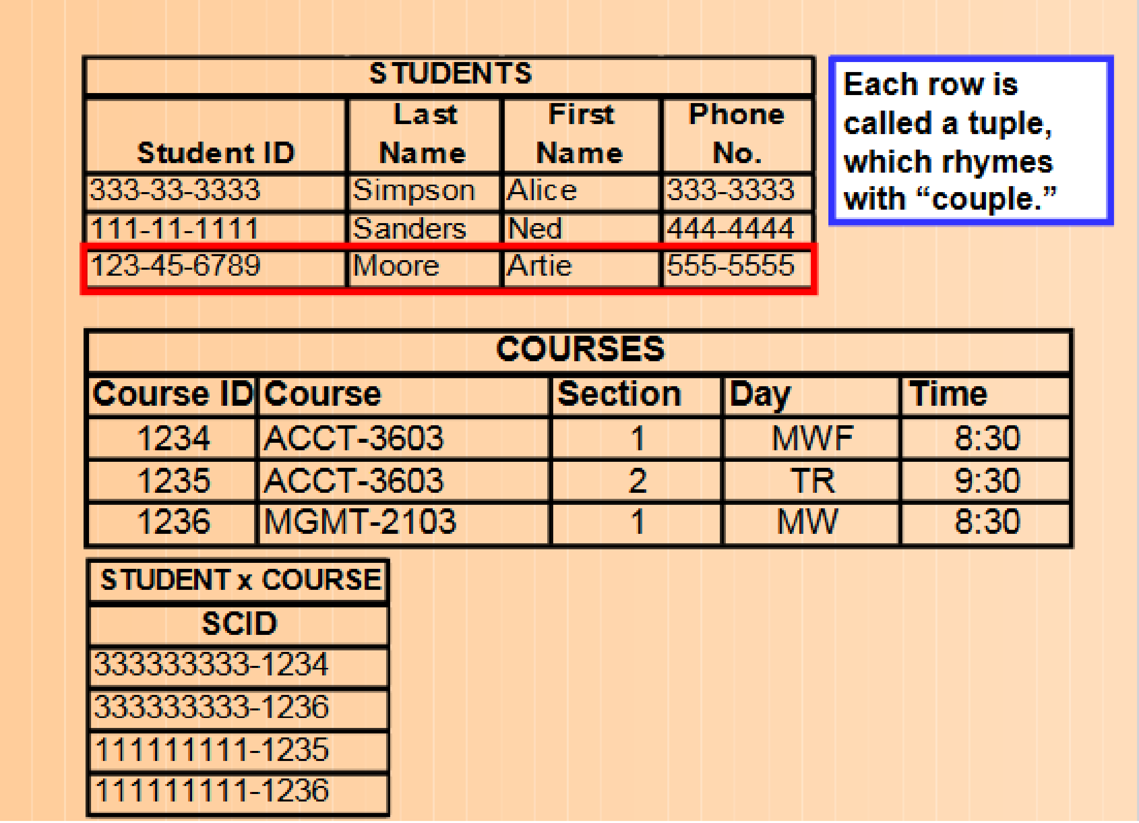
COURSES

Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE

SCID	Student ID	Course
333333333-1234	333-33-3333	1234
333333333-1236	333-33-3333	1236
111111111-1235	111-11-1111	1235
111111111-1236	111-11-1111	1235

This model only describes how the data appear in the conceptual- and external-level schemas. The data are physically stored according to the description in the internal-level schema.

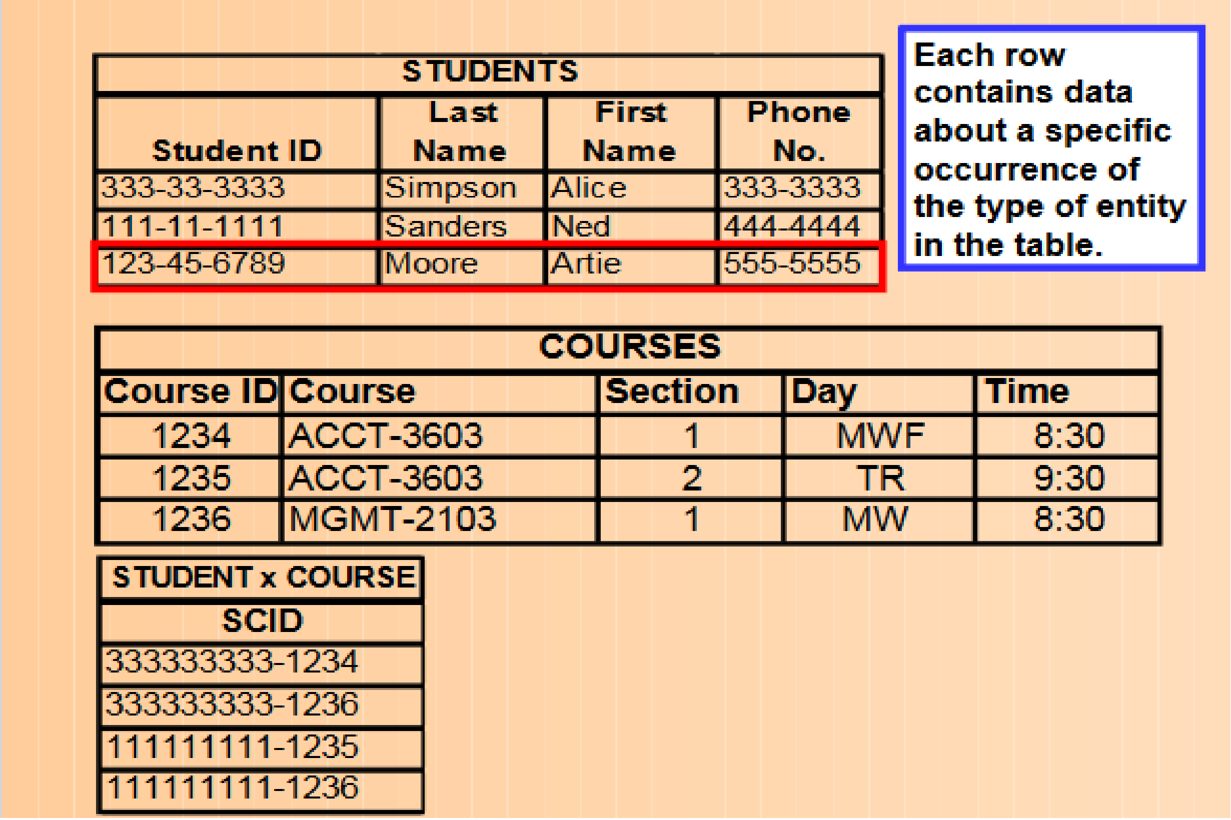


STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

Each row is called a tuple, which rhymes with “couple.”

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

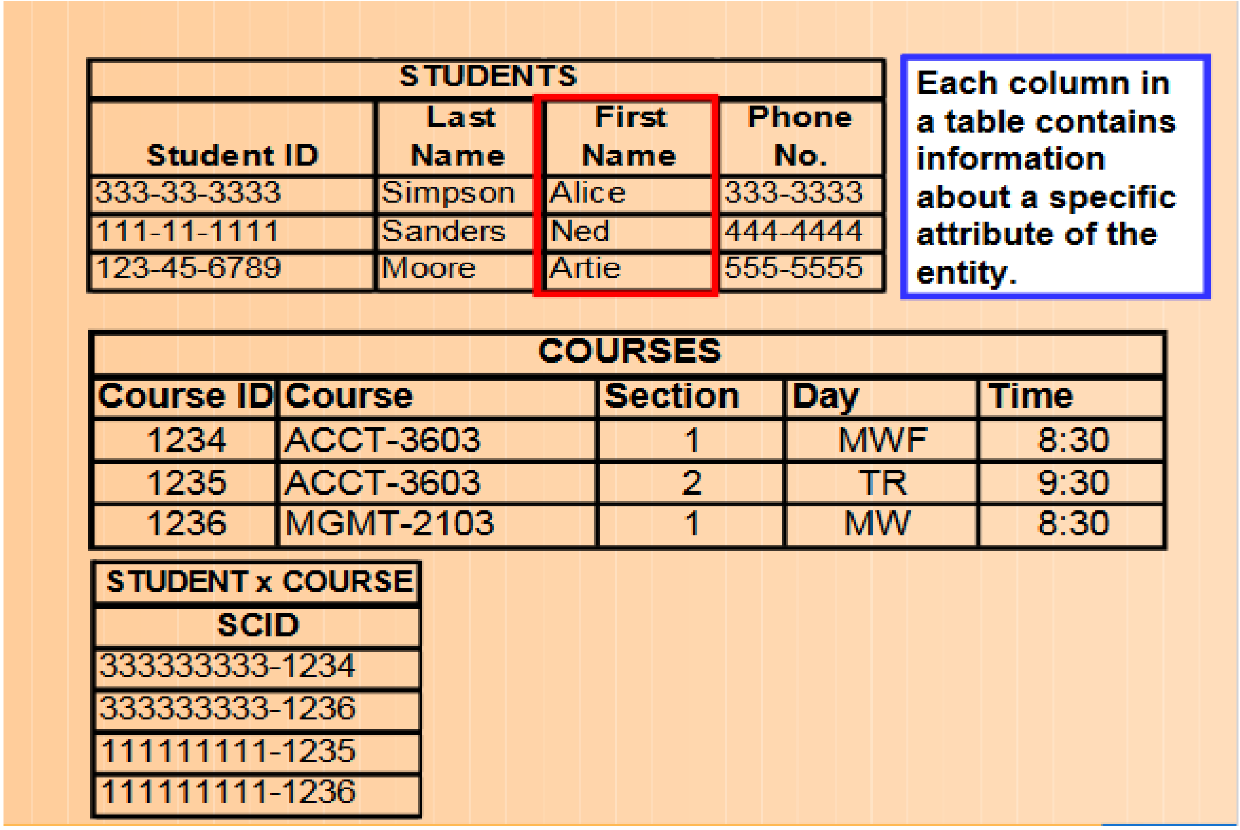


STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

Each row contains data about a specific occurrence of the type of entity in the table.

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

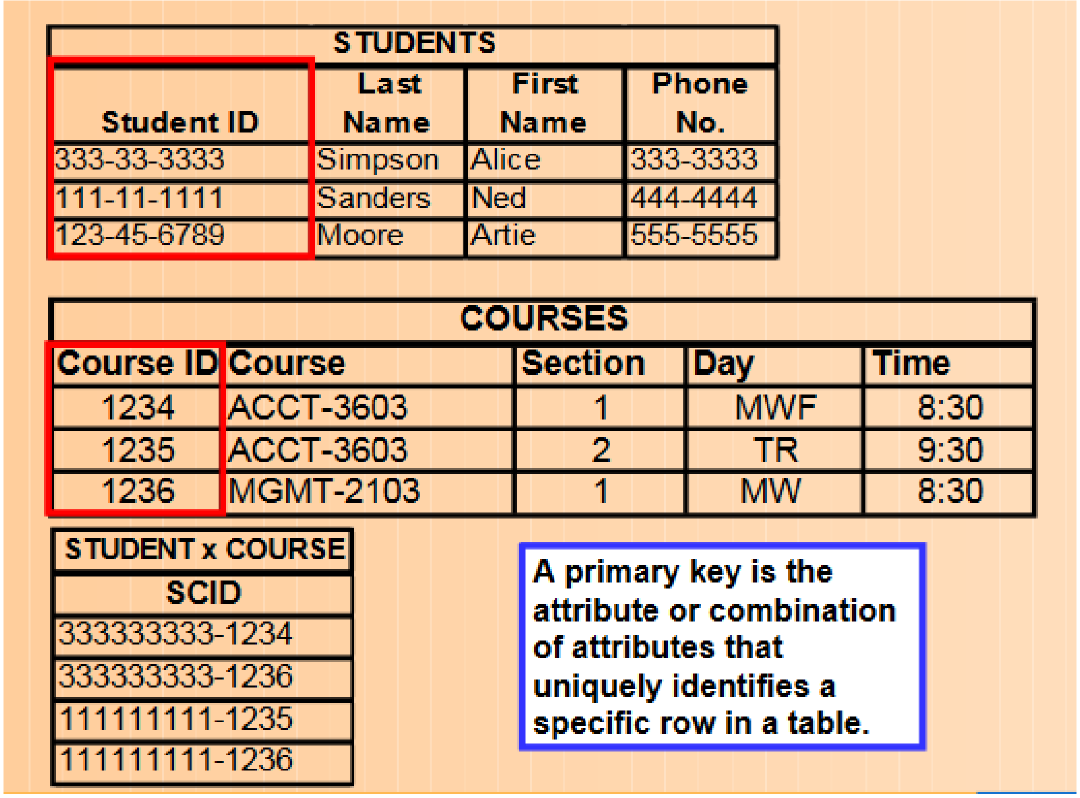


STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

Each column in a table contains information about a specific attribute of the entity.

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

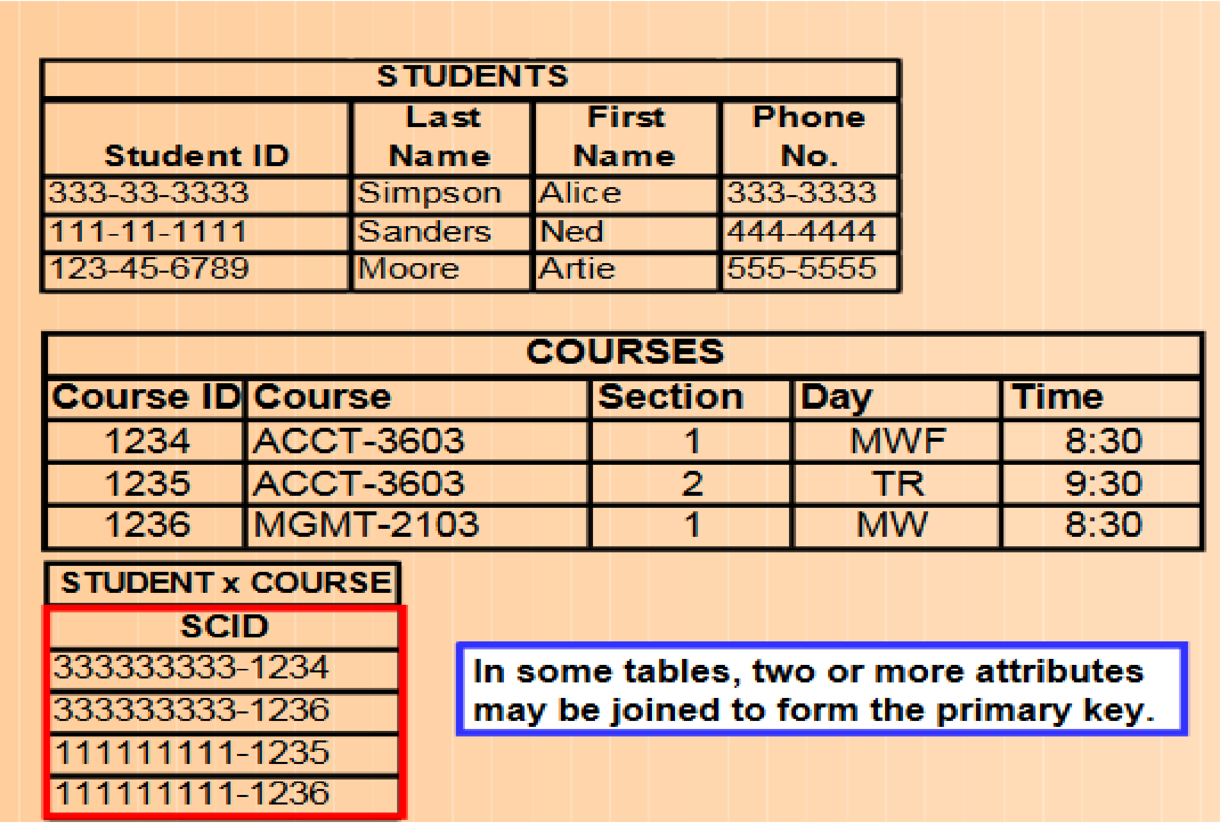


STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

A primary key is the attribute or combination of attributes that uniquely identifies a specific row in a table.

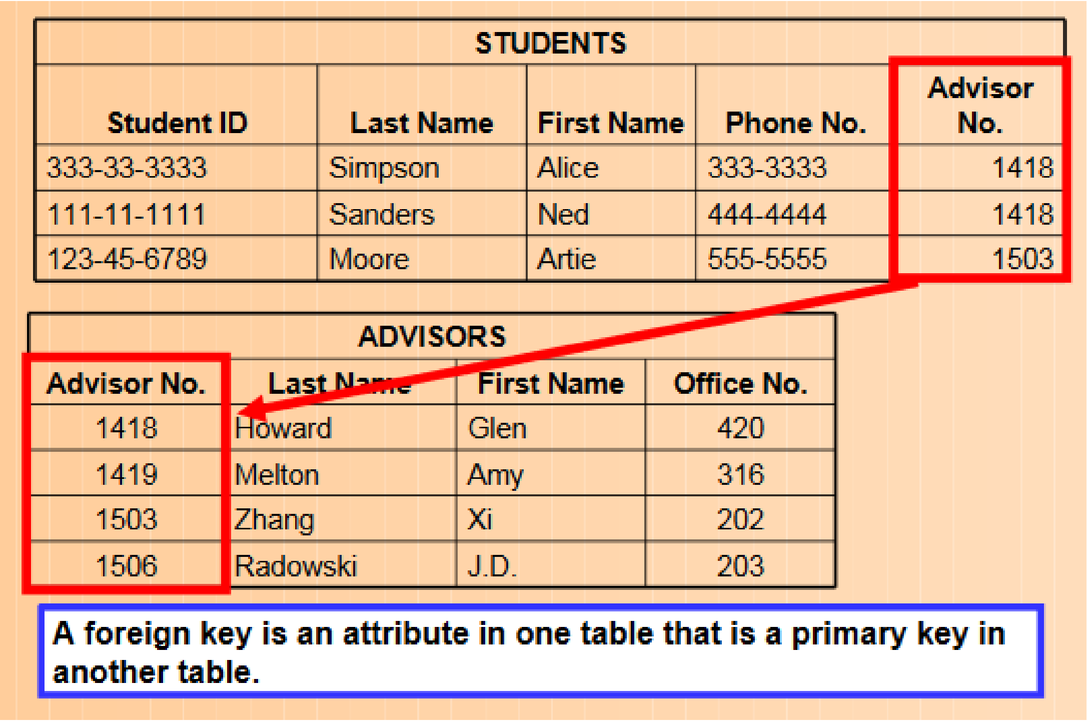


STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

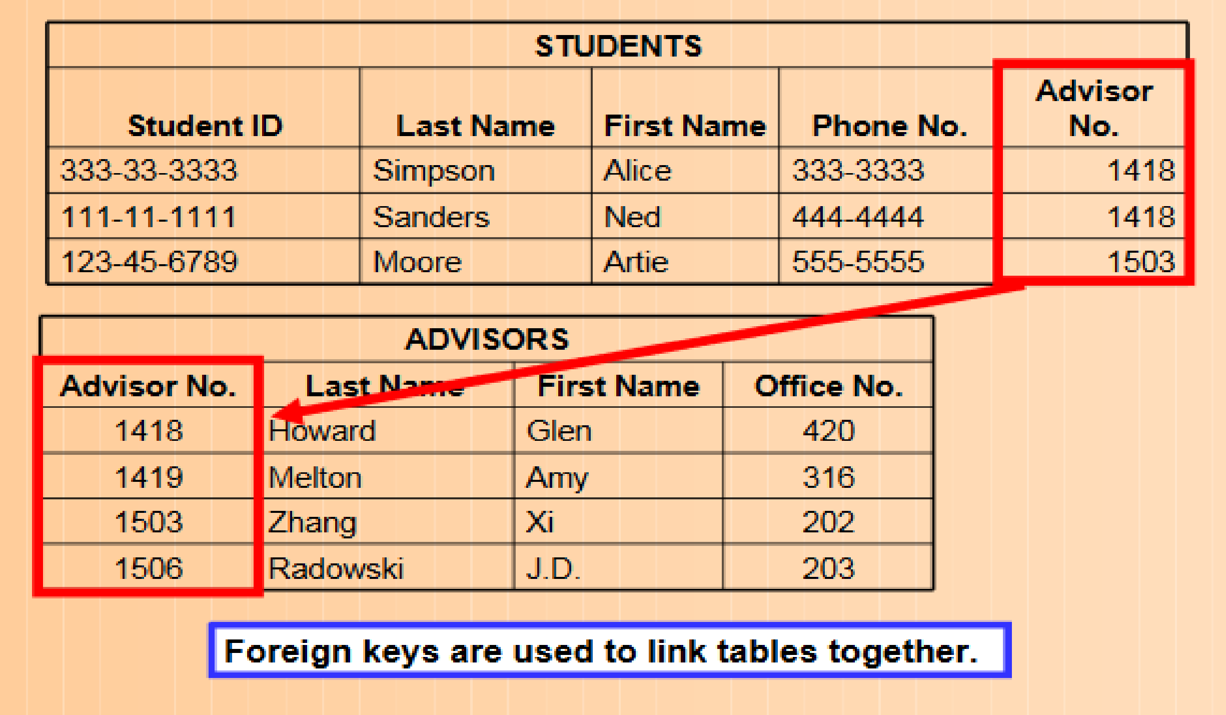
In some tables, two or more attributes may be joined to form the primary key.



STUDENTS				
Student ID	Last Name	First Name	Phone No.	Advisor No.
333-33-3333	Simpson	Alice	333-3333	1418
111-11-1111	Sanders	Ned	444-4444	1418
123-45-6789	Moore	Artie	555-5555	1503

ADVISORS			
Advisor No.	Last Name	First Name	Office No.
1418	Howard	Glen	420
1419	Melton	Amy	316
1503	Zhang	Xi	202
1506	Radowski	J.D.	203

A foreign key is an attribute in one table that is a primary key in another table.



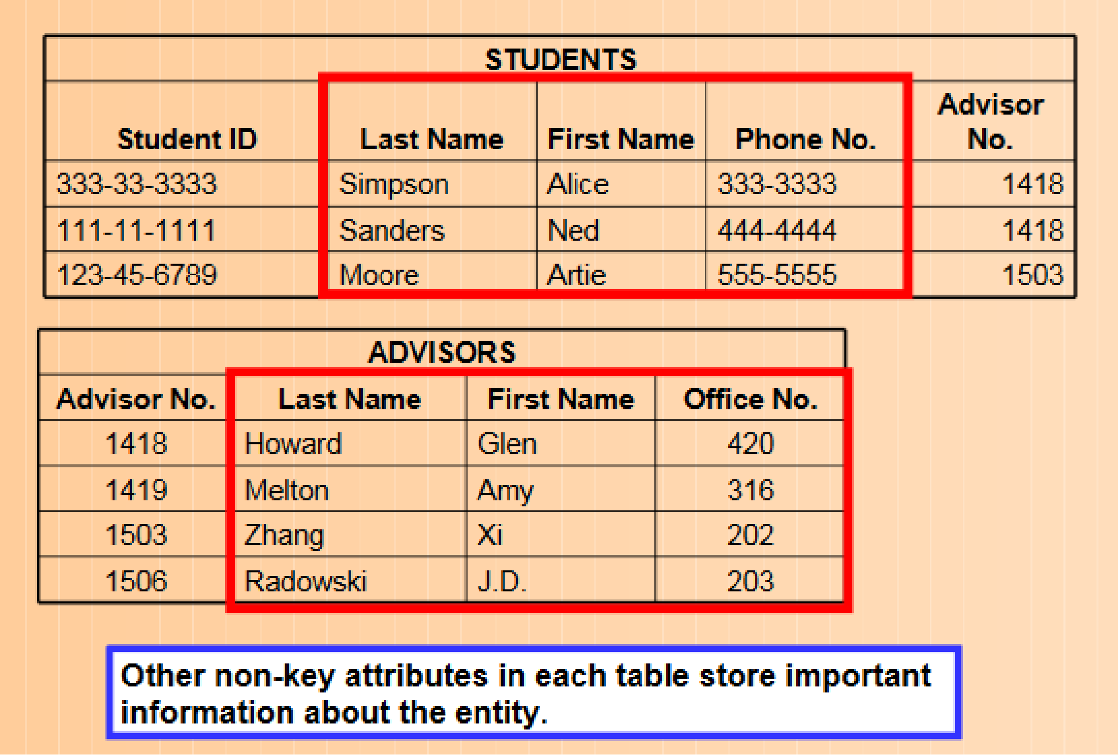
STUDENTS

Student ID	Last Name	First Name	Phone No.	Advisor No.
333-33-3333	Simpson	Alice	333-3333	1418
111-11-1111	Sanders	Ned	444-4444	1418
123-45-6789	Moore	Artie	555-5555	1503

ADVISORS

Advisor No.	Last Name	First Name	Office No.
1418	Howard	Glen	420
1419	Melton	Amy	316
1503	Zhang	Xi	202
1506	Radowski	J.D.	203

Foreign keys are used to link tables together.



STUDENTS

Student ID	Last Name	First Name	Phone No.	Advisor No.
333-33-3333	Simpson	Alice	333-3333	1418
111-11-1111	Sanders	Ned	444-4444	1418
123-45-6789	Moore	Artie	555-5555	1503

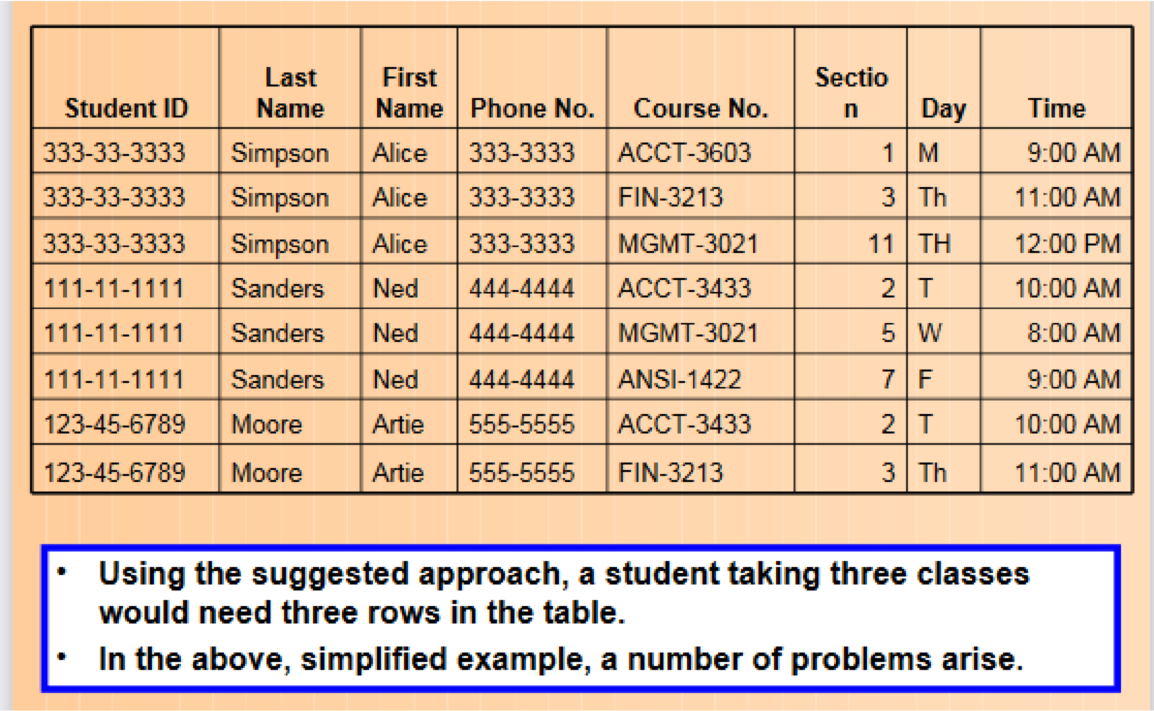
ADVISORS

Advisor No.	Last Name	First Name	Office No.
1418	Howard	Glen	420
1419	Melton	Amy	316
1503	Zhang	Xi	202
1506	Radowski	J.D.	203

Other non-key attributes in each table store important information about the entity.

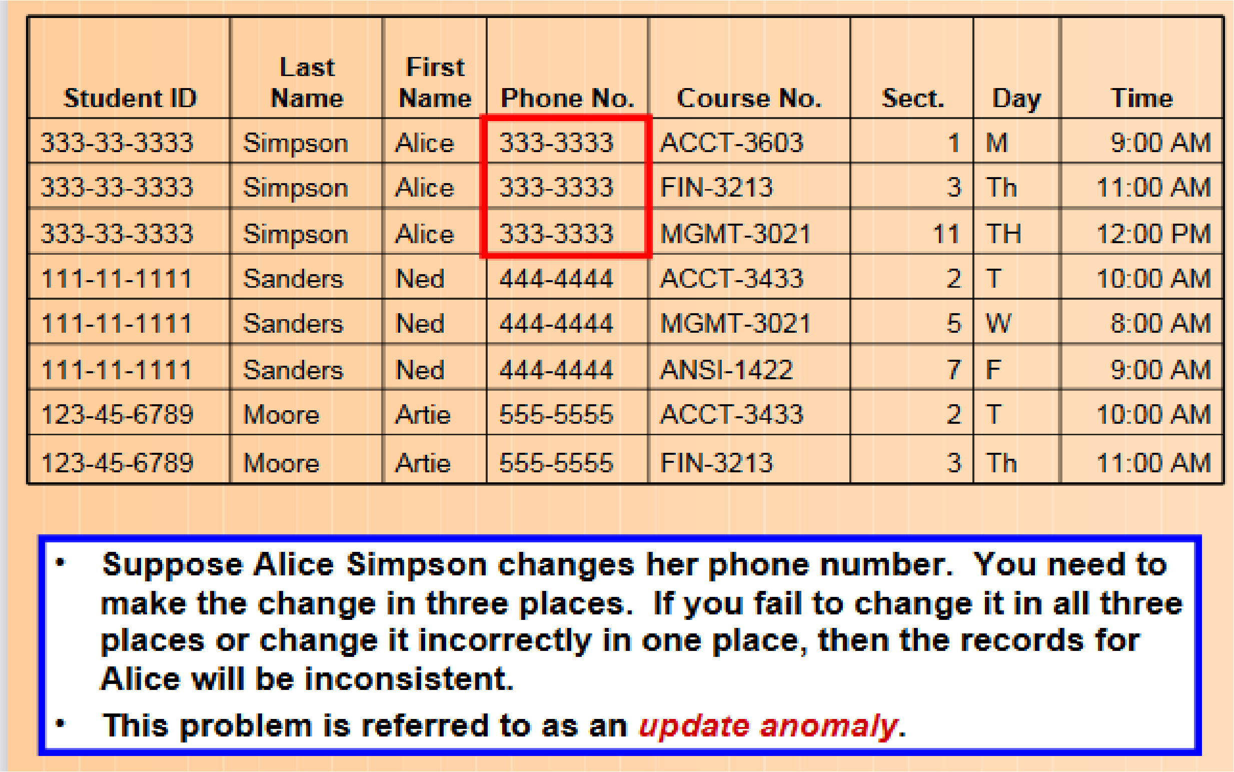
Alternatives for Storing Data

One possible alternate approach would be to store all data in one uniform table. For example, instead of separate tables for students and classes, we could store all data in one table and have a separate line for each student x class combination.



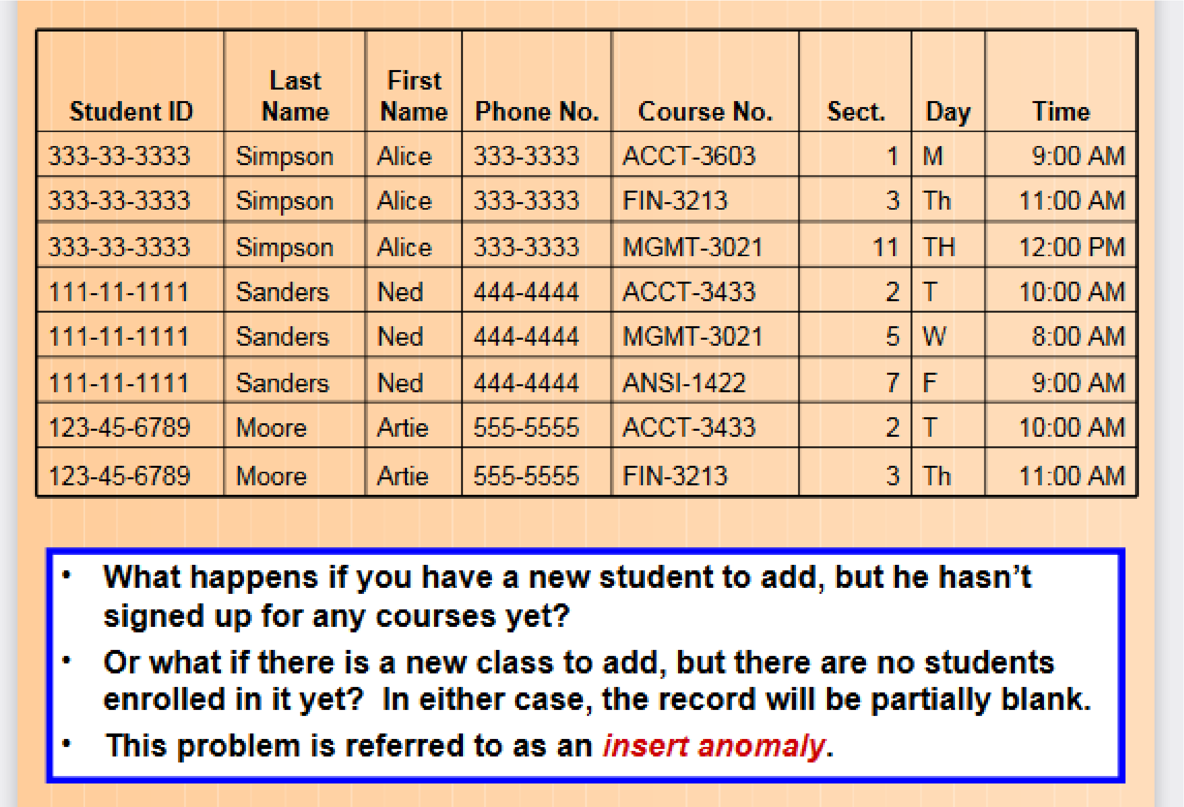
Student ID	Last Name	First Name	Phone No.	Course No.	Sectio n	Day	Time
333-33-3333	Simpson	Alice	333-3333	ACCT-3603	1	M	9:00 AM
333-33-3333	Simpson	Alice	333-3333	FIN-3213	3	Th	11:00 AM
333-33-3333	Simpson	Alice	333-3333	MGMT-3021	11	TH	12:00 PM
111-11-1111	Sanders	Ned	444-4444	ACCT-3433	2	T	10:00 AM
111-11-1111	Sanders	Ned	444-4444	MGMT-3021	5	W	8:00 AM
111-11-1111	Sanders	Ned	444-4444	ANSI-1422	7	F	9:00 AM
123-45-6789	Moore	Artie	555-5555	ACCT-3433	2	T	10:00 AM
123-45-6789	Moore	Artie	555-5555	FIN-3213	3	Th	11:00 AM

- **Using the suggested approach, a student taking three classes would need three rows in the table.**
- **In the above, simplified example, a number of problems arise.**



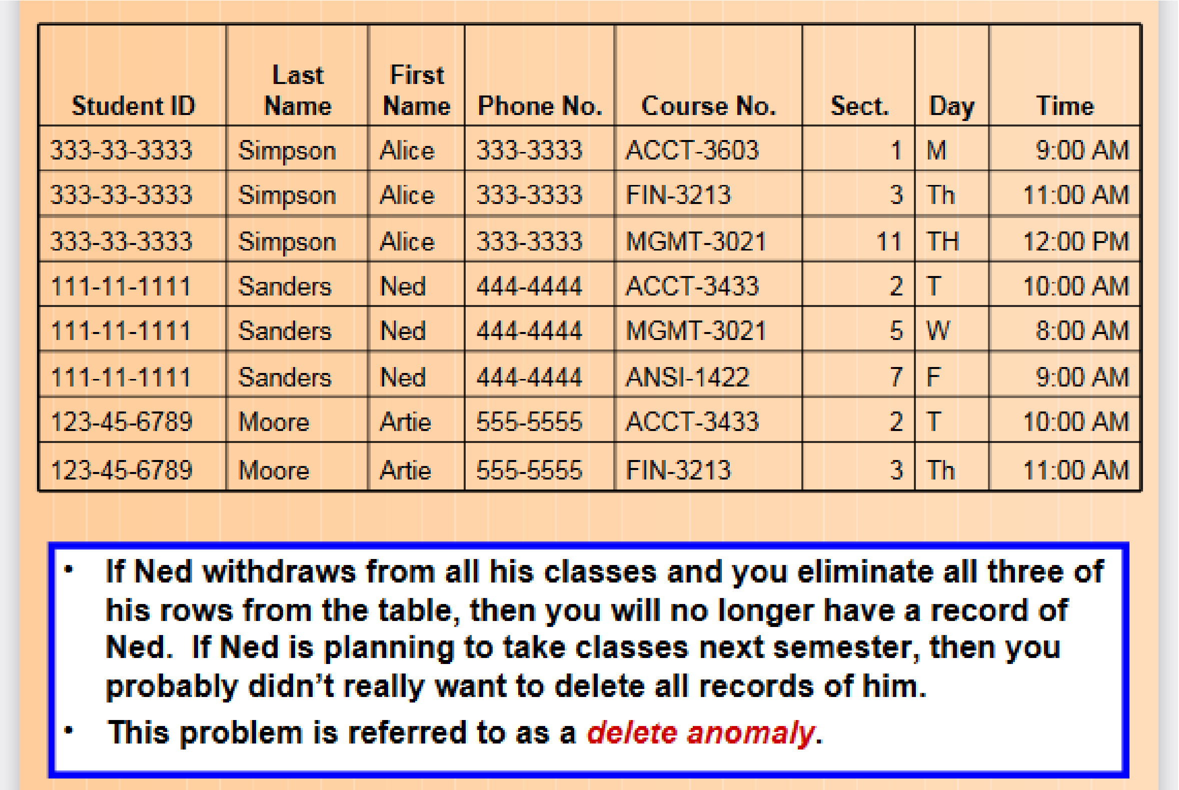
Student ID	Last Name	First Name	Phone No.	Course No.	Sect.	Day	Time
333-33-3333	Simpson	Alice	333-3333	ACCT-3603	1	M	9:00 AM
333-33-3333	Simpson	Alice	333-3333	FIN-3213	3	Th	11:00 AM
333-33-3333	Simpson	Alice	333-3333	MGMT-3021	11	TH	12:00 PM
111-11-1111	Sanders	Ned	444-4444	ACCT-3433	2	T	10:00 AM
111-11-1111	Sanders	Ned	444-4444	MGMT-3021	5	W	8:00 AM
111-11-1111	Sanders	Ned	444-4444	ANSI-1422	7	F	9:00 AM
123-45-6789	Moore	Artie	555-5555	ACCT-3433	2	T	10:00 AM
123-45-6789	Moore	Artie	555-5555	FIN-3213	3	Th	11:00 AM

- **Suppose Alice Simpson changes her phone number. You need to make the change in three places. If you fail to change it in all three places or change it incorrectly in one place, then the records for Alice will be inconsistent.**
- **This problem is referred to as an *update anomaly*.**



Student ID	Last Name	First Name	Phone No.	Course No.	Sect.	Day	Time
333-33-3333	Simpson	Alice	333-3333	ACCT-3603	1	M	9:00 AM
333-33-3333	Simpson	Alice	333-3333	FIN-3213	3	Th	11:00 AM
333-33-3333	Simpson	Alice	333-3333	MGMT-3021	11	TH	12:00 PM
111-11-1111	Sanders	Ned	444-4444	ACCT-3433	2	T	10:00 AM
111-11-1111	Sanders	Ned	444-4444	MGMT-3021	5	W	8:00 AM
111-11-1111	Sanders	Ned	444-4444	ANSI-1422	7	F	9:00 AM
123-45-6789	Moore	Artie	555-5555	ACCT-3433	2	T	10:00 AM
123-45-6789	Moore	Artie	555-5555	FIN-3213	3	Th	11:00 AM

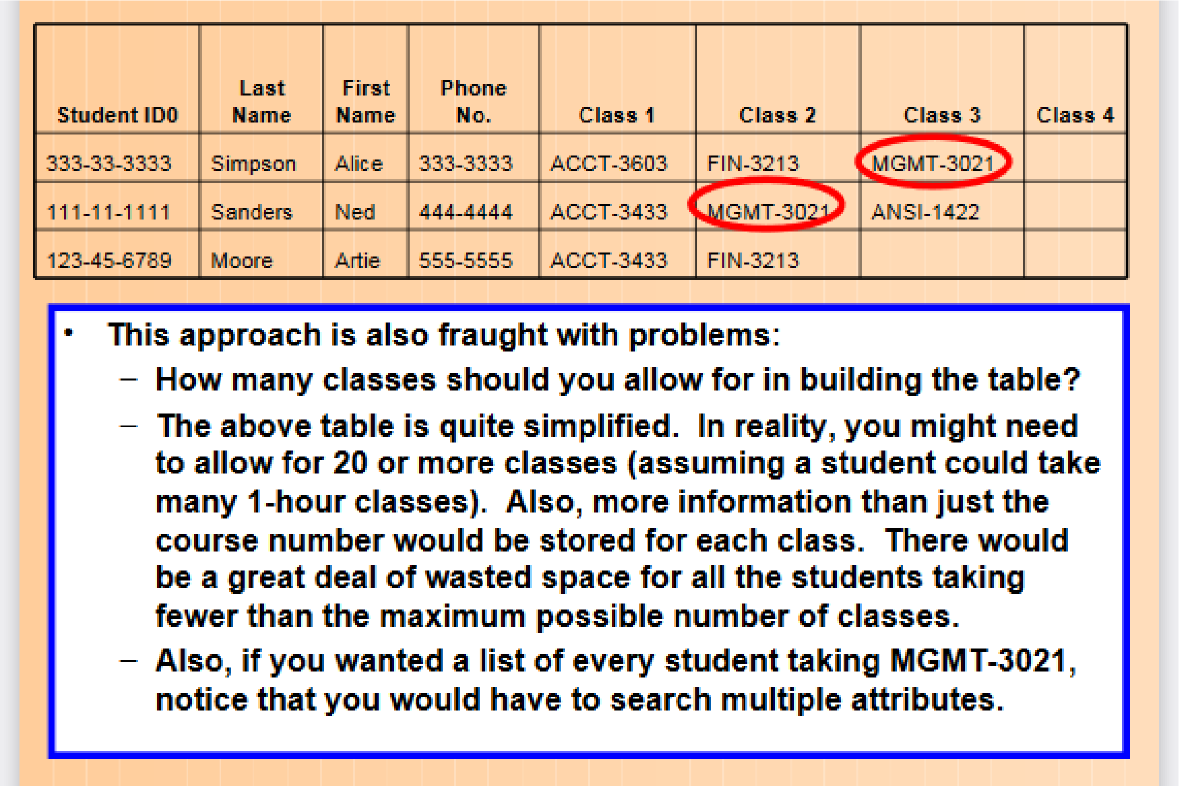
- **What happens if you have a new student to add, but he hasn't signed up for any courses yet?**
- **Or what if there is a new class to add, but there are no students enrolled in it yet? In either case, the record will be partially blank.**
- **This problem is referred to as an *insert anomaly*.**



Student ID	Last Name	First Name	Phone No.	Course No.	Sect.	Day	Time
333-33-3333	Simpson	Alice	333-3333	ACCT-3603	1	M	9:00 AM
333-33-3333	Simpson	Alice	333-3333	FIN-3213	3	Th	11:00 AM
333-33-3333	Simpson	Alice	333-3333	MGMT-3021	11	TH	12:00 PM
111-11-1111	Sanders	Ned	444-4444	ACCT-3433	2	T	10:00 AM
111-11-1111	Sanders	Ned	444-4444	MGMT-3021	5	W	8:00 AM
111-11-1111	Sanders	Ned	444-4444	ANSI-1422	7	F	9:00 AM
123-45-6789	Moore	Artie	555-5555	ACCT-3433	2	T	10:00 AM
123-45-6789	Moore	Artie	555-5555	FIN-3213	3	Th	11:00 AM

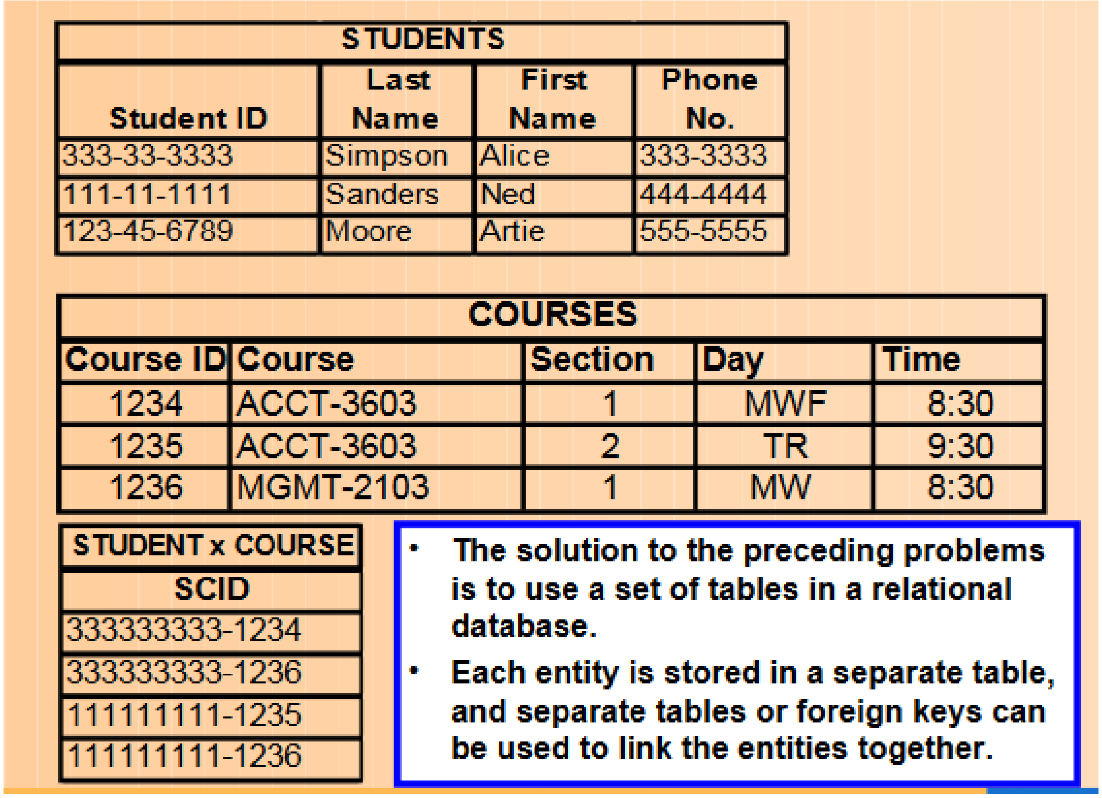
- **If Ned withdraws from all his classes and you eliminate all three of his rows from the table, then you will no longer have a record of Ned. If Ned is planning to take classes next semester, then you probably didn't really want to delete all records of him.**
- **This problem is referred to as a *delete anomaly*.**

Alternatives for Storing Data–Another possible approach would be to store each student in one row of the table and create multiple columns to accommodate each class that he is taking.



Student ID0	Last Name	First Name	Phone No.	Class 1	Class 2	Class 3	Class 4
333-33-3333	Simpson	Alice	333-3333	ACCT-3603	FIN-3213	MGMT-3021	
111-11-1111	Sanders	Ned	444-4444	ACCT-3433	MGMT-3021	ANSI-1422	
123-45-6789	Moore	Artie	555-5555	ACCT-3433	FIN-3213		

- **This approach is also fraught with problems:**
  - **How many classes should you allow for in building the table?**
  - **The above table is quite simplified. In reality, you might need to allow for 20 or more classes (assuming a student could take many 1-hour classes). Also, more information than just the course number would be stored for each class. There would be a great deal of wasted space for all the students taking fewer than the maximum possible number of classes.**
  - **Also, if you wanted a list of every student taking MGMT-3021, notice that you would have to search multiple attributes.**



STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

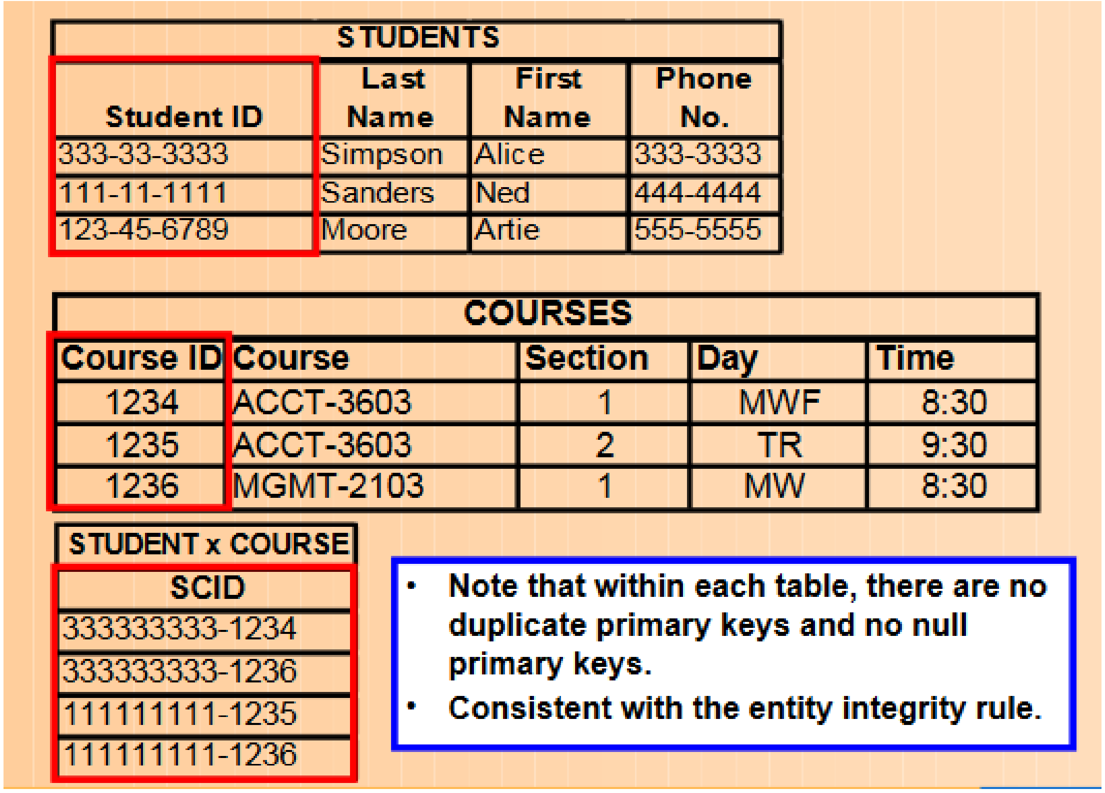
STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

- **The solution to the preceding problems is to use a set of tables in a relational database.**
- **Each entity is stored in a separate table, and separate tables or foreign keys can be used to link the entities together.**

2.2.4 Basic Requirements of a Relational Database

Every column in a row must be single valued. In other words, every cell can have one and only one value. In the student table, you couldn't have an attribute named "Phone Number" if a student could have multiple phone numbers. There might be an attribute named "local phone number" and an attribute named "permanent phone number." You could not have an attribute named "Class" in the student table, because a student could take multiple classes.

- The primary key cannot be null.
- The primary key uniquely identifies a specific row in the table, so it cannot be null, and it must be unique for every record. This rule is referred to as the ***entity integrity rule***.



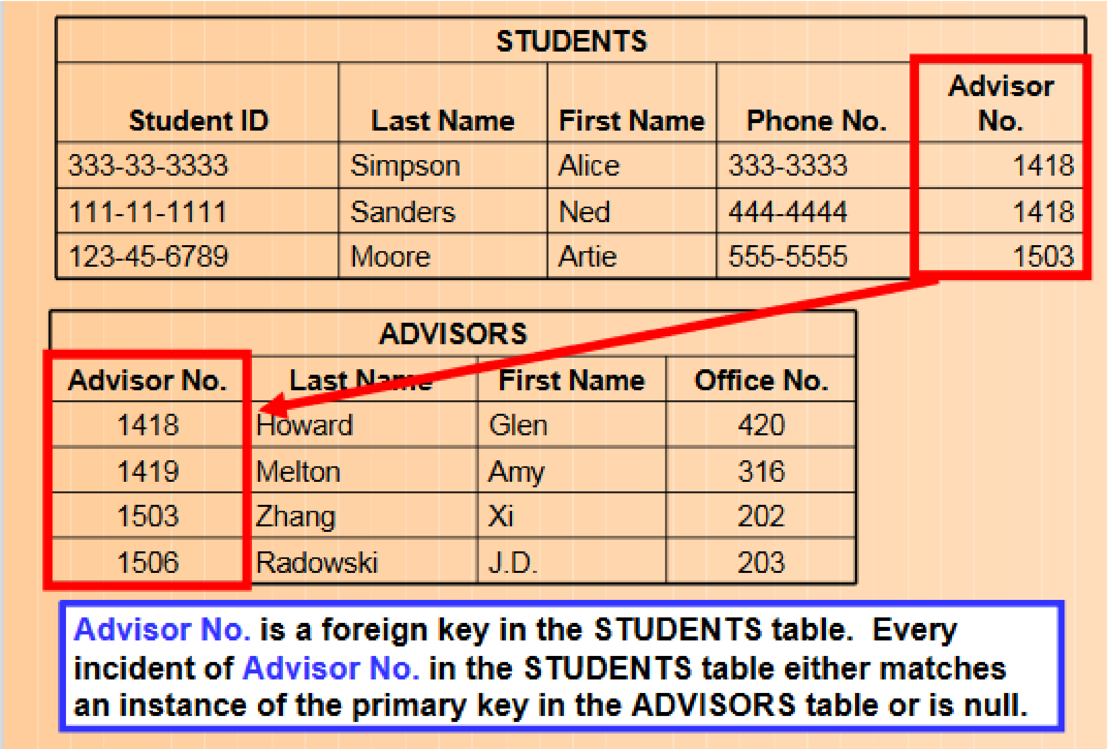
STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

- **Note that within each table, there are no duplicate primary keys and no null primary keys.**
- **Consistent with the entity integrity rule.**

A foreign key must either be null or correspond to the value of a primary key in another table. This rule is referred to as the referential integrity rule. The rule is necessary because foreign keys are used to link rows in one table to rows in another table.



STUDENTS				
Student ID	Last Name	First Name	Phone No.	Advisor No.
333-33-3333	Simpson	Alice	333-3333	1418
111-11-1111	Sanders	Ned	444-4444	1418
123-45-6789	Moore	Artie	555-5555	1503

ADVISORS			
Advisor No.	Last Name	First Name	Office No.
1418	Howard	Glen	420
1419	Melton	Amy	316
1503	Zhang	Xi	202
1506	Radowski	J.D.	203

Advisor No. is a foreign key in the STUDENTS table. Every incident of Advisor No. in the STUDENTS table either matches an instance of the primary key in the ADVISORS table or is null.

All non-key attributes in a table should describe a characteristic of the object identified by the primary key. Could nationality be a non-key attribute in the student table? Could advisor's nationality be a non-key attribute in the student table? The preceding four constraints produce a well-structured (normalized) database in which;

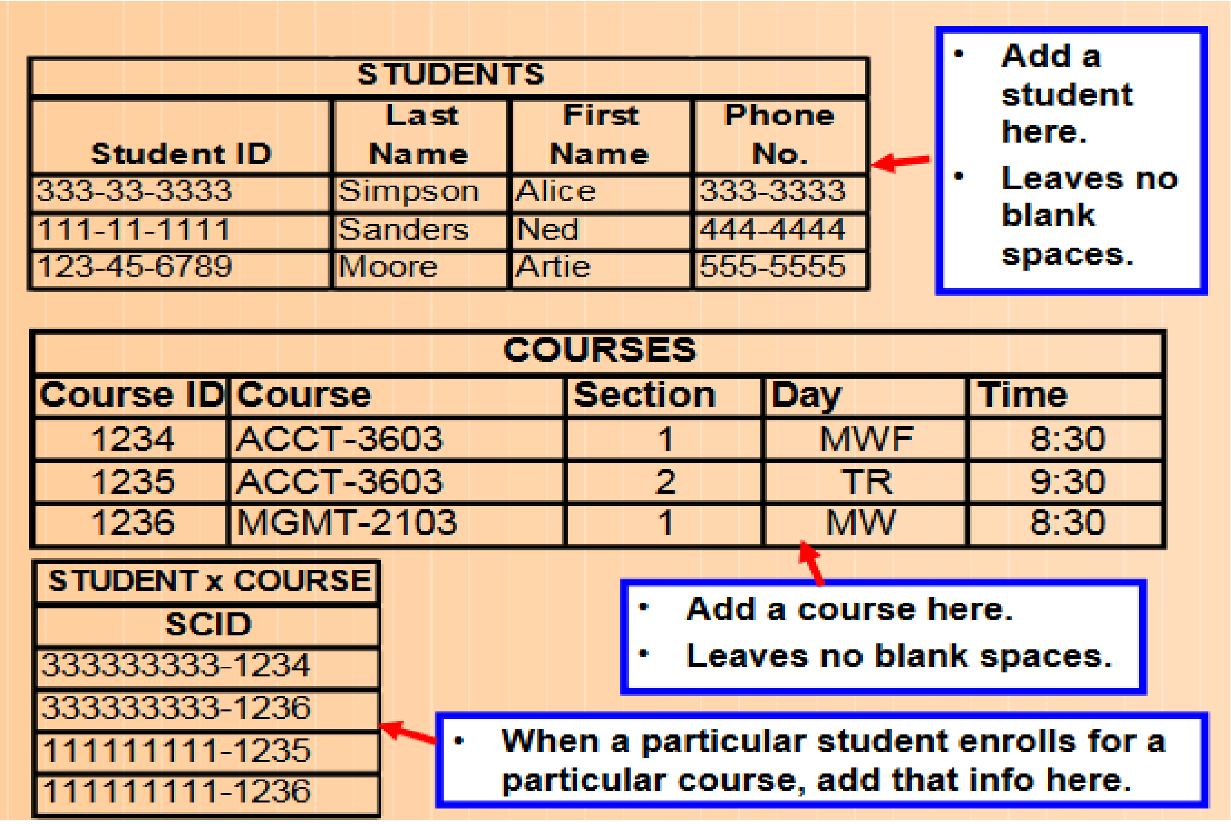
- Data are consistent.
- Redundancy is minimized and controlled.

In a normalized database, attributes appear multiple times only when they function as foreign keys. The referential integrity rule ensures there will be no update anomaly problem with foreign keys.

An important feature is that data about various things of interest (entities) are stored in separate tables. Makes it easier to add new data to the system. You add a new student by adding a row to the student table. You add a new course by adding a row to the course table. Means you can add a student even if he hasn't signed up for any courses. And you can add a class even if no students are yet enrolled in it.

Makes it easy to avoid the insert anomaly

Space is also used more efficiently than in the other schemes. There should be no blank rows or attributes.



STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

- Add a student here.
- Leaves no blank spaces.

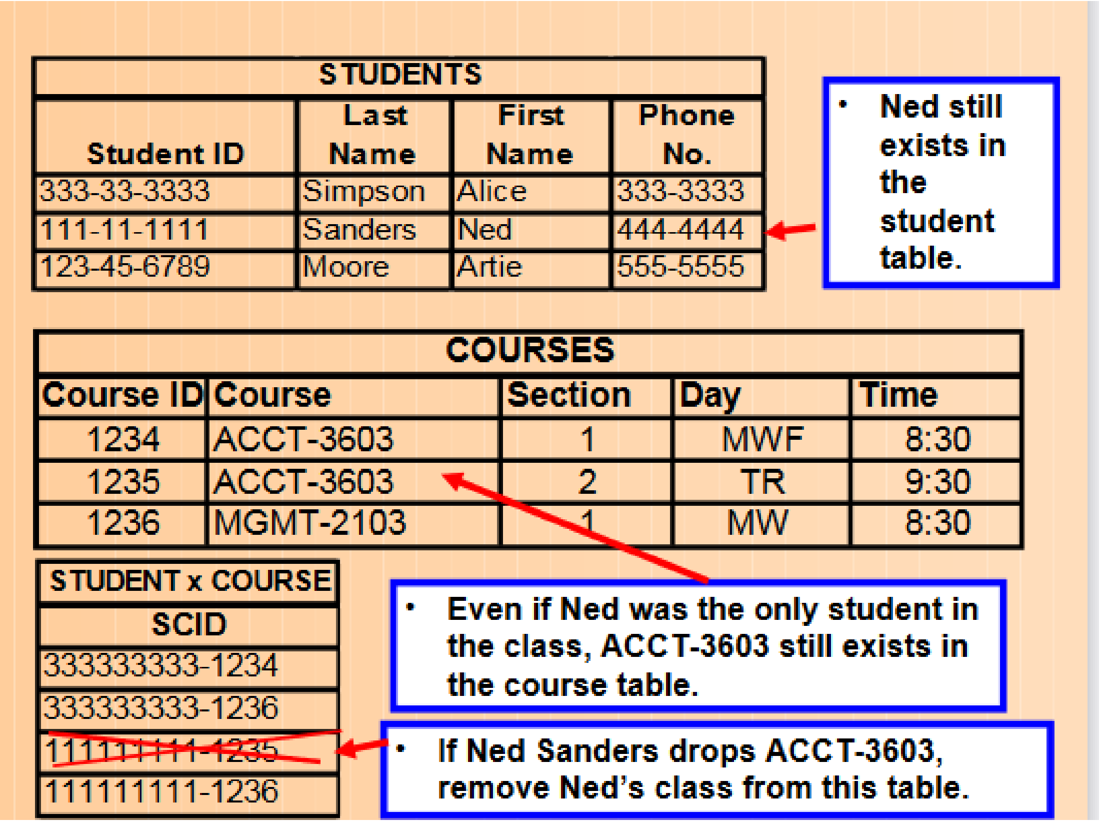
COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

- Add a course here.
- Leaves no blank spaces.

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
111111111-1235
111111111-1236

- When a particular student enrolls for a particular course, add that info here.

Deletion of a class for a student would cause the elimination of one record in the student x class table.–The student still exists in the student table.–The class still exists in the class table.–Avoids the delete anomaly



STUDENTS			
Student ID	Last Name	First Name	Phone No.
333-33-3333	Simpson	Alice	333-3333
111-11-1111	Sanders	Ned	444-4444
123-45-6789	Moore	Artie	555-5555

- Ned still exists in the student table.

COURSES				
Course ID	Course	Section	Day	Time
1234	ACCT-3603	1	MWF	8:30
1235	ACCT-3603	2	TR	9:30
1236	MGMT-2103	1	MW	8:30

STUDENT x COURSE
SCID
333333333-1234
333333333-1236
~~111111111-1235~~
111111111-1236

- Even if Ned was the only student in the class, ACCT-3603 still exists in the course table.

- If Ned Sanders drops ACCT-3603, remove Ned's class from this table.

There are two basic ways to design well-structured relational databases.–Normalization–Semantic data modeling

- **i.** Normalization
- **ii.** Semantic Data Modelling

i. *Normalization*

Starts with the assumption that everything is initially stored in one large table. A set of rules is followed to decompose that initial table into a set of normalized tables. Objective is to produce a set of tables in third-normal form (3NF) because such tables are free of update, insert, and delete anomalies. Approach is beyond the scope of this book but can be found in any database textbook.

ii. *Semantic data modeling*

Database designer uses knowledge about how business processes typically work and the information needs associated with transaction processing to draw a graphical picture of what should be included in the database. The resulting graphic is used to create a set of relational tables that are in 3NF.

Advantages over simply following normalization rules:

Semantic data modeling uses the designer's knowledge about business processes and practices; it therefore facilitates efficient design of transaction processing databases. The resulting graphical model explicitly represents information about the organization's business processes and policies and facilitates communication with intended users.

2.2.5 Creating Relational Database Queries

Databases store data for people and organizations. To retrieve the data, you query the database and its tables. Try these on your own and hand it to your instructor in class to see.

2.3 DATABASE SYSTEMS AND THE FUTURE OF ACCOUNTING

Database systems may profoundly affect the fundamental nature of accounting: May lead to abandonment of double-entry accounting, because the redundancy of the double entry is not necessary in computer data processing. May also alter the nature of external reporting. ***Example***: External users could have access to the company's database and manipulate the data to meet their own reporting needs.

The use of accounting information in decision making will be enhanced by: Powerful querying capabilities that accompany database packages. The ability to accommodate multiple views of the same underlying phenomenon. The ability to integrate financial and operational data.

Accountants must become knowledgeable about databases so they can participate in developing the AIS of the future. They must help ensure that adequate controls are included to safeguard the data and assure its reliability.

SUMMARY

You've learned how databases differ from file-based legacy systems. You've learned why databases are important and what advantages they offer. You've learned how the logical and physical views of a database differ. You've learned about fundamental concepts of database systems such as DBMS, schemas, the data dictionary, and DBMS languages. You've learned what a relational database is and how it organizes data. You've learned how tables are structured to properly store data in a relational database.

Unit 3

E-BUSINESS

Objectives of the unit

At the end of the unit you will be able to:

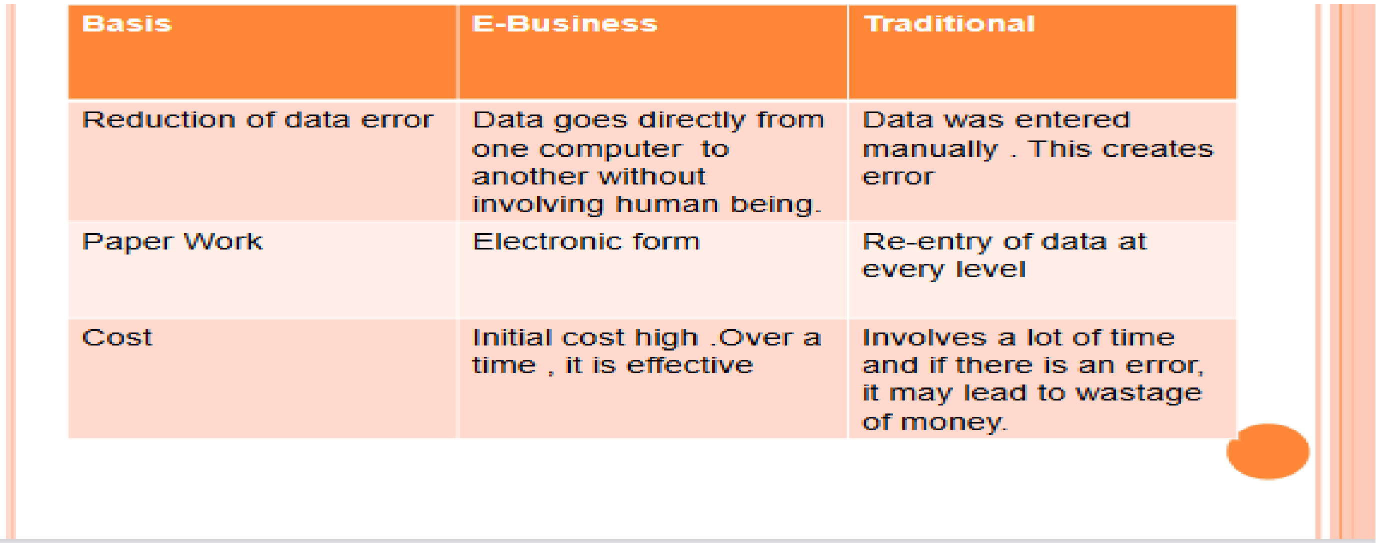
i. Know the importance of E-Business in an organization and why it must be adopted
ii. Learn the difference of e-business and e-commerce
iii. Know the functioning electronic data interchange
iv. Learn and have knowledge on Enterprise resource planning
v. Have knowledge on business transactions

3.0 INTRODUCTION TO E-BUSINESS.

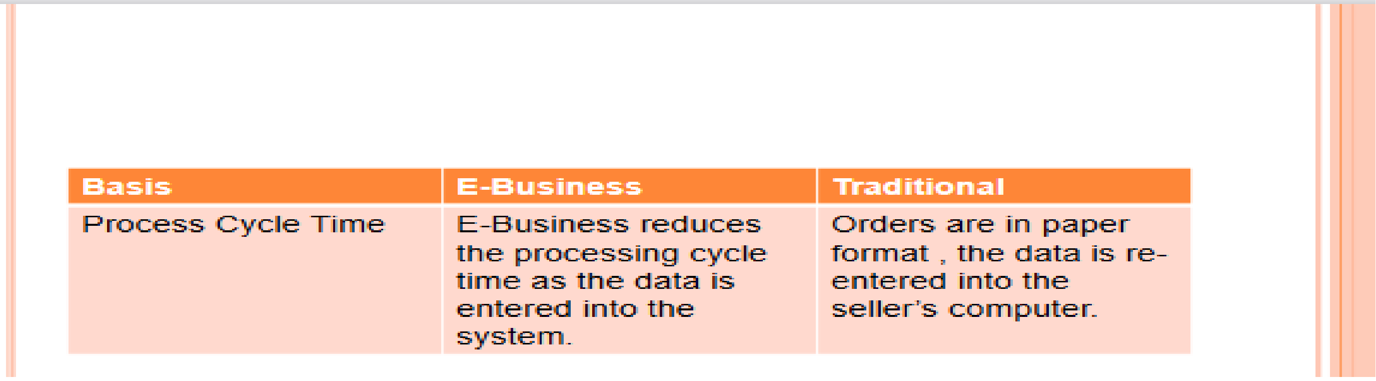
- Deals with the buying and selling of information, products and services through the computer network. Business activity which uses electronic medium. E Business (e-Business), or Electronic Business, is the administration of conducting business via the Internet. This would include the buying and selling of goods and services, along with providing technical or customer support through the Internet.

3.1 ORIGIN OF E-BUSINESS

- 1950s: Computers were used to process and store records of internal transactions. But information between various business continued to be exchanged on paper.
- 1960s: exchanging transaction information on punched cards or magnetic tapes. Later, transferring data over telephones, instead of shipping punched cards or magnetic tapes.
- 1970s: Introduction of Electronic Data Interchange (EDI) between the banks over a secured private network changed the financial market.
- 1972: IBM used the term 'e-business'. E-Business became widespread within companies in the form of electronic messaging technologies i.e., EDI and E-mail.
- Next slide shows E-business vs Traditional Business.



Basis	E-Business	Traditional
Reduction of data error	Data goes directly from one computer to another without involving human being.	Data was entered manually . This creates error
Paper Work	Electronic form	Re-entry of data at every level
Cost	Initial cost high .Over a time , it is effective	Involves a lot of time and if there is an error, it may lead to wastage of money.



Basis	E-Business	Traditional
Process Cycle Time	E-Business reduces the processing cycle time as the data is entered into the system.	Orders are in paper format , the data is re-entered into the seller's computer.

3.1.1 a. Advantages of E-Business

- All time processing
- Better service
- Removing mediators
- Time saving
- Enhanced speed and accuracy of a product
- Cost saving of the product
- Reduces paper work
- Fast dissipation of information
- Global reach

3.1.1 b. Disadvantages of E-Business

- Lack of customer awareness
- Small Businessmen do not want to take any extra burden
- Legal formalities
- It is not free
- Security problems
- Customer satisfaction problems
- Data integrity problems

3.1.2 PREREQUISITES FOR E-BUSINESS PROCEDURE

- A Commercial website

- Products or services
- Shopping Carts or Purchase Order forms
- Current credit card account that will be accepted on e-payment
- An online payment gateway
- A secure socket layer –secure the gateway

3.1.3 E-BUSINESS AREAS

- Tourism and Travel
- Banking sector
- Health care sector
- Stock sector
- Financial sector

3.1.4 DEFINITION OF E-COMMERCE

- E-commerce is an abbreviation used for electronic commerce. It is the process through which the buying, selling, dealing, ordering and paying for the goods and services are done over the internet.
- In this type of online commercial transaction, the seller can communicate with the buyer without having face to face interaction.
- Some examples of real world application of e-commerce are online banking, online shopping, online ticket booking.

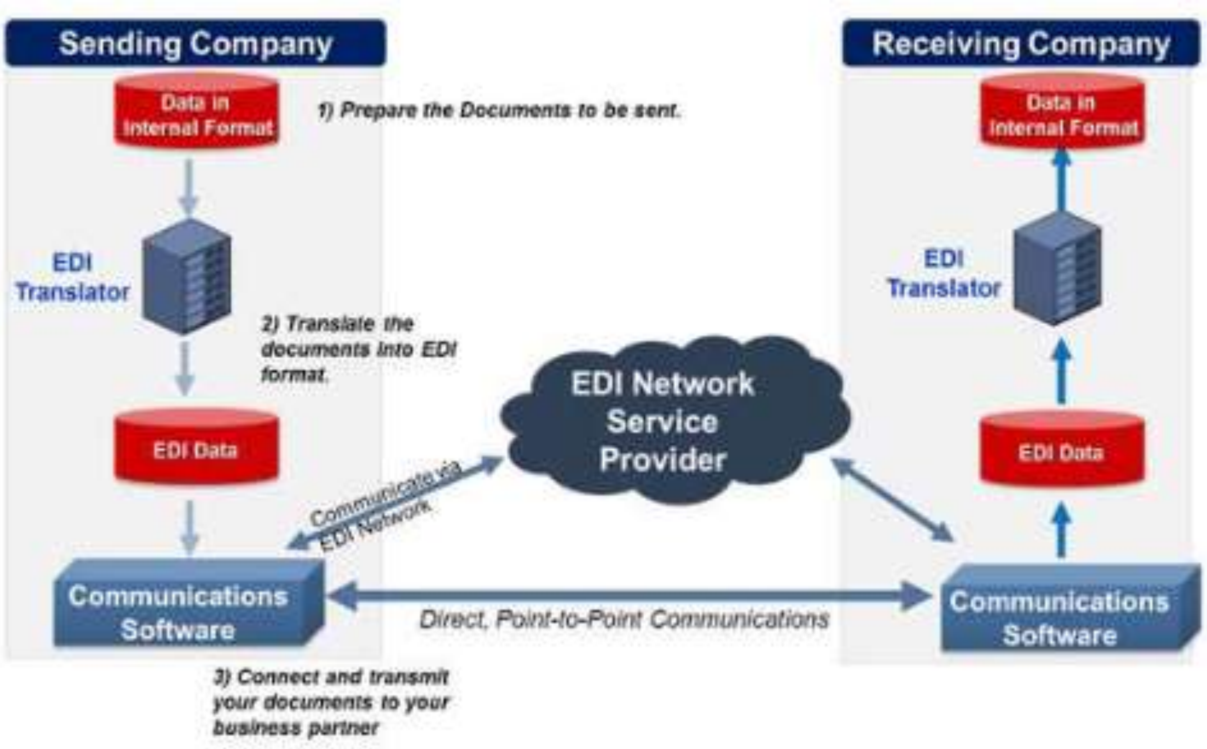
3.1.5 KEY DIFFERENCES BETWEEN E-COMMERCE AND E-BUSINESS

- Buying and Selling of goods and services through the internet is known as e-commerce.
- Unlike e-business, which is an electronic presence of a business, by which all the business activities are conducted through the internet.
- E-commerce is a major component of e-business.
- E-commerce includes transactions which are related to money, but e-business, includes monetary as well as allied activities.
- E-commerce has an extroverted approach that covers customers, suppliers, distributors, etc. On the other hand, e-business has an ambiverted approach that covers internal as well as external processes.
- E-commerce requires a website that can represent the business. Conversely, e-business requires a website, Customer Relationship Management and Enterprise Resource Planning for running business over the internet.
- E-commerce uses the internet to connect with the rest of the world. In contrast to e-business, internet, intranet and extranet are used for connecting with the parties.

3.2 EDI (ELECTRONIC DATA INTERCHANGE)

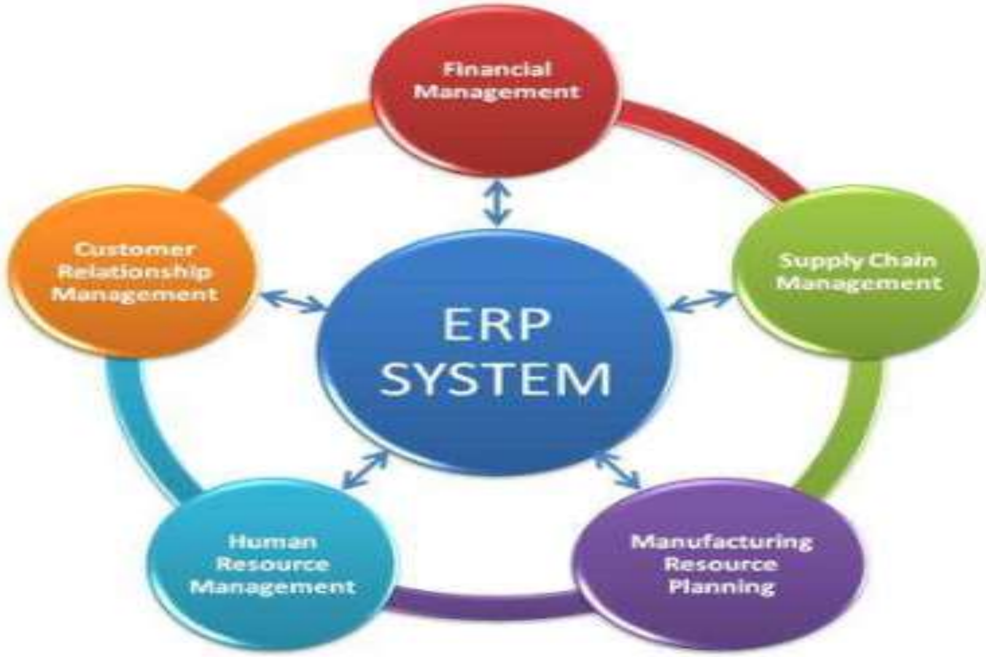
- EDI (Electronic Data Interchange) is the transfer of data from one computer system to another by standardized message formatting, without the need for human intervention.
- EDI permits multiple companies --possibly in different countries --to exchange documents electronically

3.2.1 WORKING OF EDI


Sending Company
Receiving Company
Data in Internal Format
1) Prepare the Documents to be sent.
EDI Translator
2) Translate the documents into EDI format.
EDI Data
EDI Network Service Provider
Communicate via EDI Network
Communications Software
Direct, Point-to-Point Communications
3) Connect and transmit your documents to your business partner
Data in Internal Format
EDI Translator
EDI Data
Communications Software

3.3 ERP (ENTERPRISE RESOURCE PLANNING)

- Enterprise resource planning (ERP) is a category of business-management software—typically a suite of integrated applications—that an organization can use to collect, store, manage and interpret data from many business activities, including:
- *Product planning, cost*
- *Manufacturing or service delivery*
- *Marketing and sales*
- *Inventory management*
- *Shipping and payment*

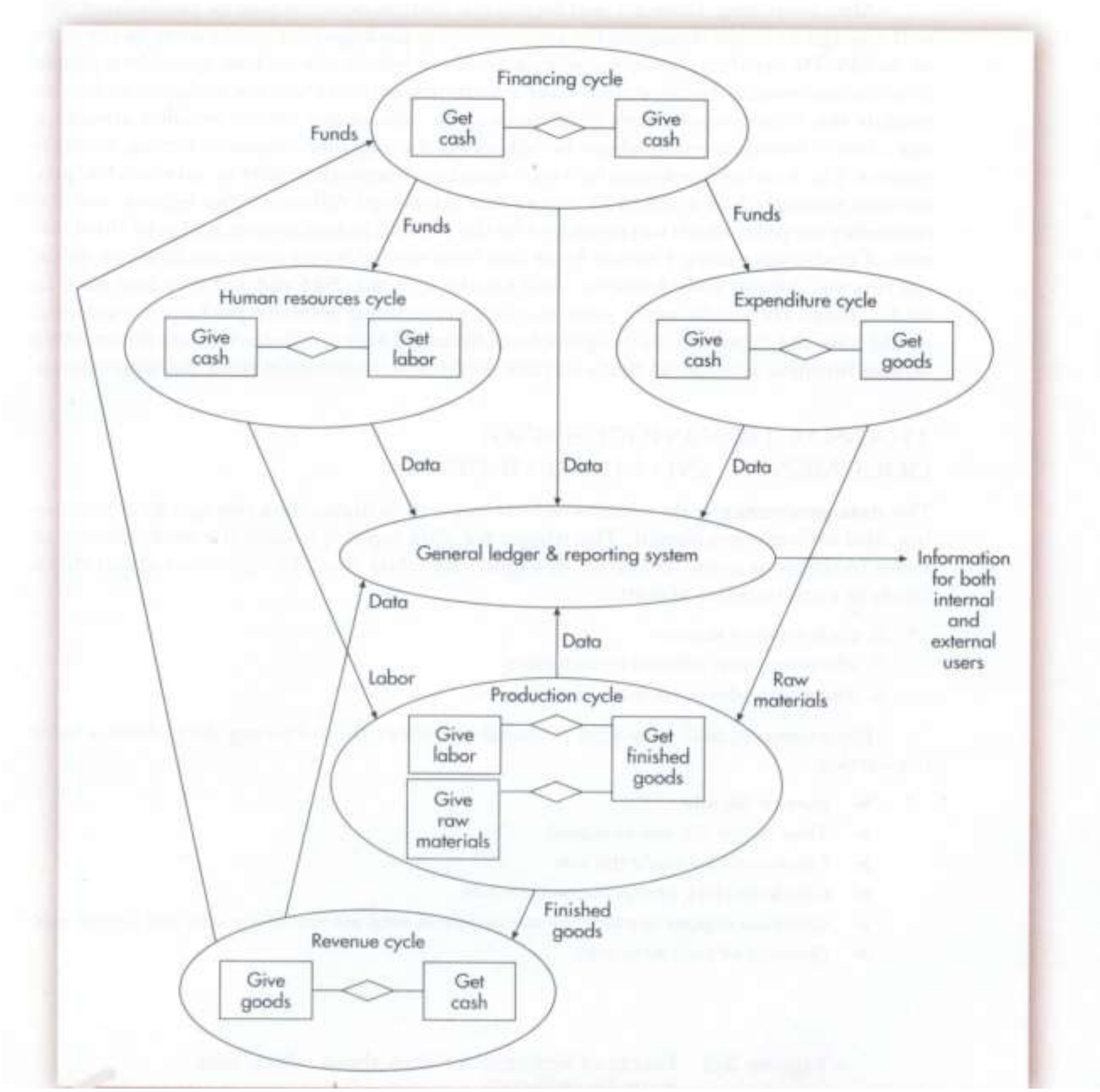

Financial Management
Customer Relationship Management
ERP SYSTEM
Supply Chain Management
Human Resource Management
Manufacturing Resource Planning

3.4 BUSINESS TRANSACTION

Businesses deals in buying or procuring, selling and offering services, collecting receivable and making payables, they also transit goods and services all the financial cycle. This are the business transactions that takes place. Each transactions goes round all the accounting period as the company is in existence. We are going to discuss these business transaction cycles in brief before getting into an elaborative study to each.

a) Transaction Cycles

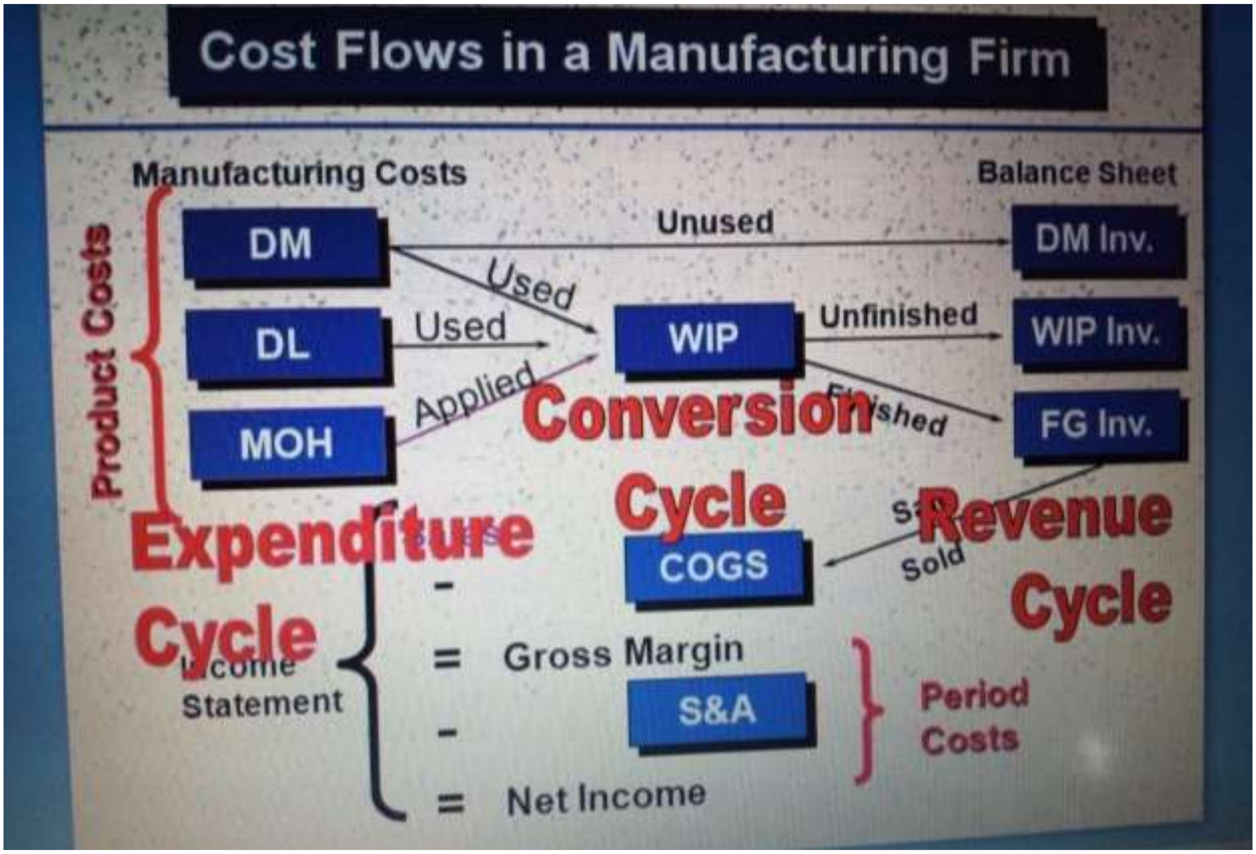
- A transaction processing cycle combines one or more types of transactions having related features or similar objectives. A transaction cycle consists of a set of transactions leading to the recognition of a major economic event on the financial statements
- It is through the study of transaction cycles that we gain a clear view of a firm's processing framework. (See Figure 2-1 below)



-

Figure 2-1: the AIS and its subsystems. Source: adopted from Arizona state university.
We can have something familiar to this

Cost Flows in a Manufacturing Firm



Cost Flows in a Manufacturing Firm

Manufacturing Costs

Balance Sheet

Product Costs

DM

DL

MOH

Unused

Used

Used

Applied

WIP

Unfinished

Finished

DM Inv.

WIP Inv.

FG Inv.

Sold

COGS

Expenditure Cycle

Conversion Cycle

Revenue Cycle

Income Statement

-

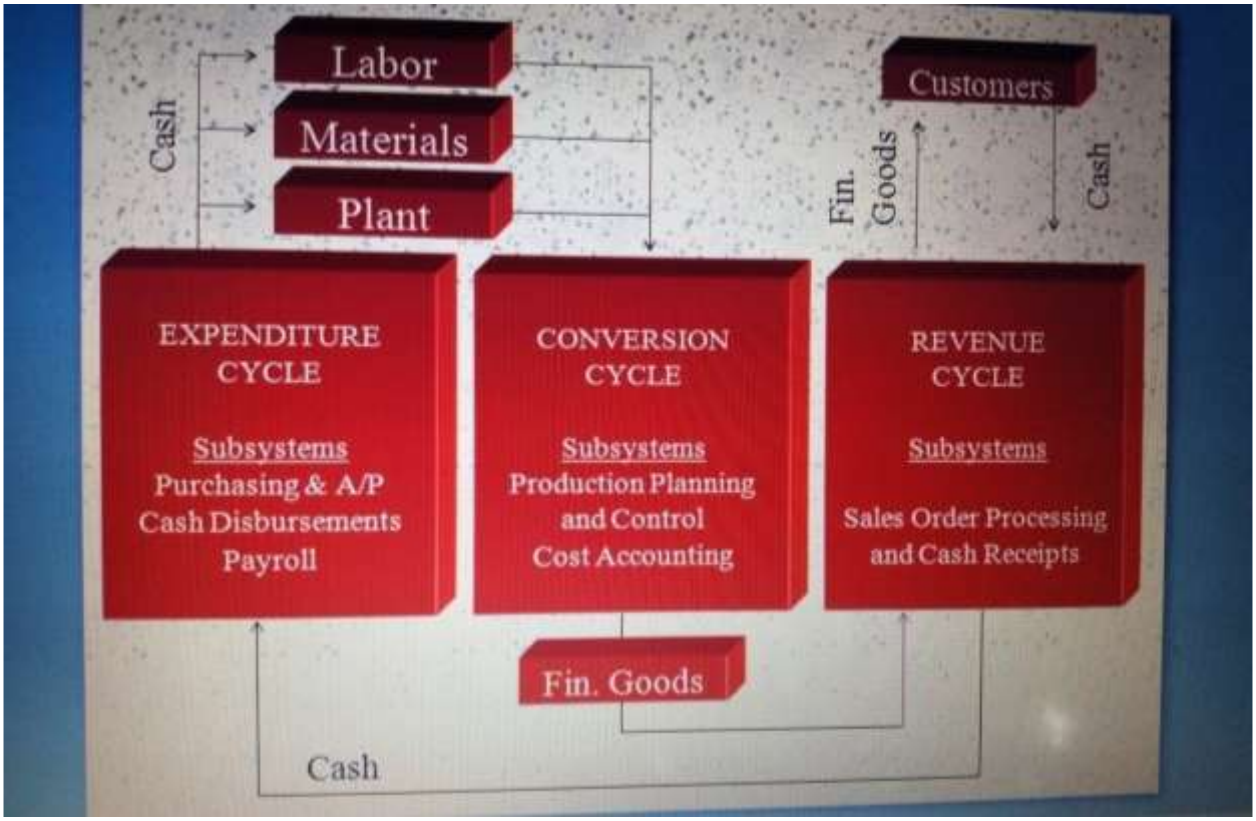
= Gross Margin

S&A

-

= Net Income

Period Costs



Cash

Labor

Materials

Plant

Customers

Fin. Goods

Cash

EXPENDITURE CYCLE

Subsystems
Purchasing & A/P
Cash Disbursements
Payroll

CONVERSION CYCLE

Subsystems
Production Planning and Control
Cost Accounting

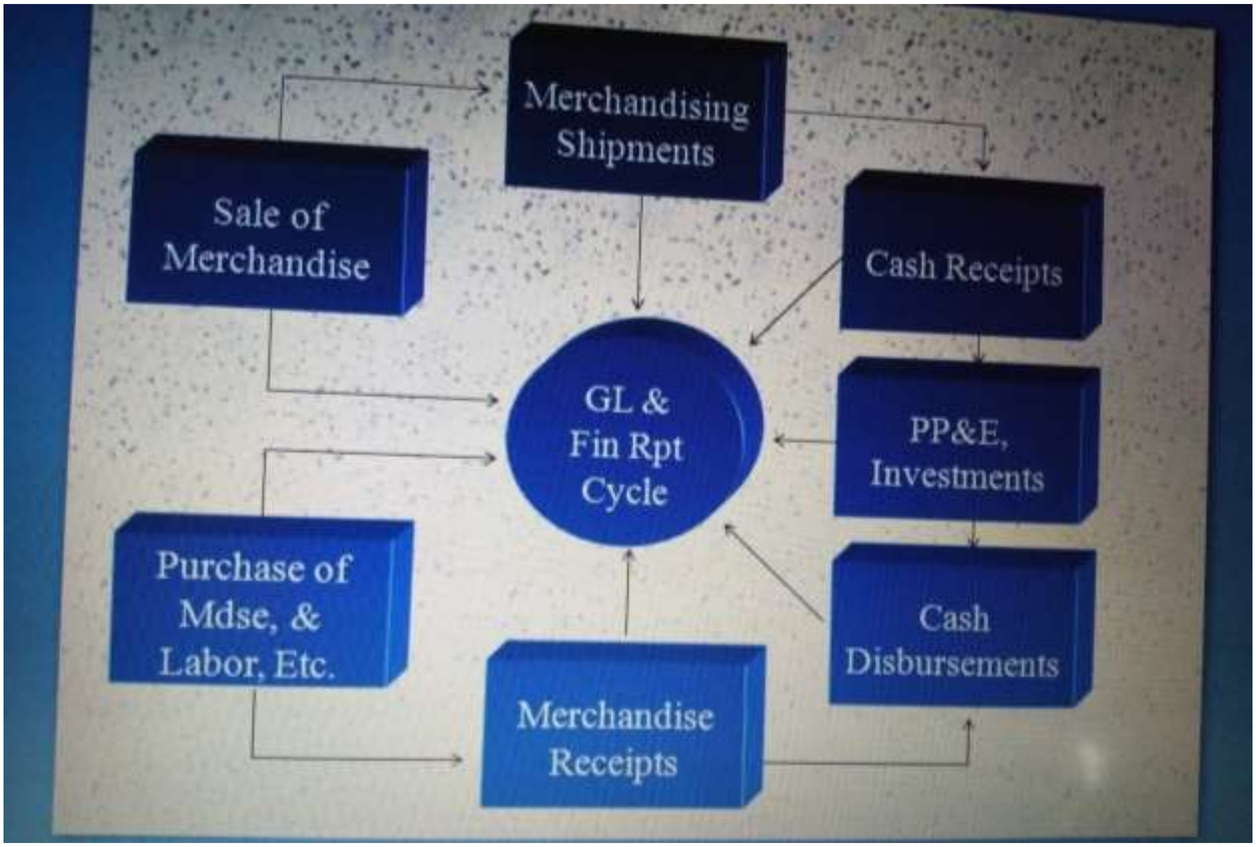
REVENUE CYCLE

Subsystems
Sales Order Processing and Cash Receipts

Fin. Goods

Cash

An other approach



3.4.1 REVENUE CYCLE, SALES, CASH COLLECTIONS.

- Includes transactions surrounding the recognition of revenue.
  - Sales
  - Accounts Receivable
  - Inventory (some)
  - General Ledger (some)

Capturing and recording of customer orders;
Shipment of the goods and the recording of the cost of goods sold.
The billing process and the recording of sales and accounts receivable;
The capturing and recording of cash receipts.

3.4.2 EXPENDITURE CYCLE, PURCHASING, CASH DEBT.

Includes the transactions surrounding the recognition of expenditures.	
■ Purchases ■ Accounts Payable ■ Cash Disbursements	■ Inventory (some) ■ General Ledger (some)

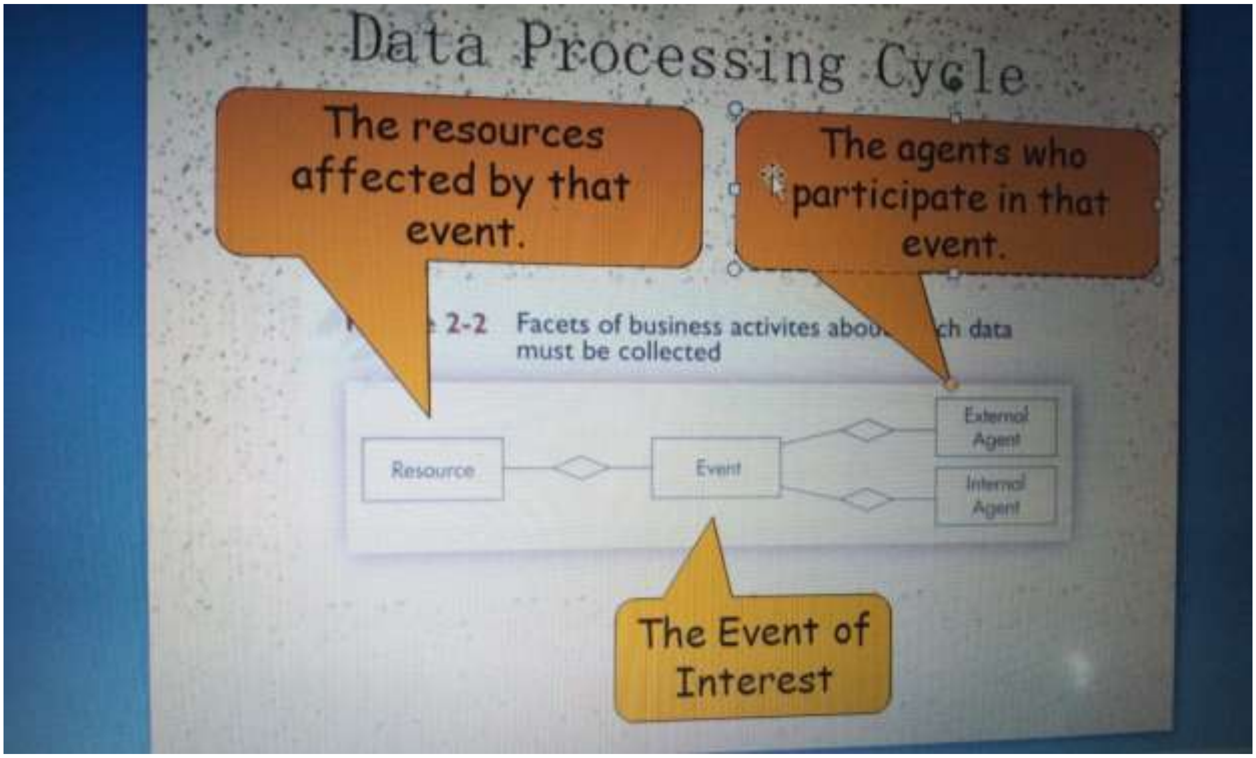
- The preparation and recording of purchase orders;
- The receipt of goods and the recording of the cost of inventory;
- The receipt of vendor invoices and the recording of accounts payable;
- The preparation and recording of cash disbursements.

- The cycle also includes the preparation of employee paychecks and the recording of payroll activities.

<u>AIS function #1</u>

i. <u>Collect</u> and <u>store</u> data about the organization’s business activities and transactions efficiently and effectively
ii. Capture transaction data on source documents.
iii. Record transaction data in journals, which present a chronological record of what occurred.
iv. Post data from journals to ledgers, which sort data by account type.

3.4.3 Data Processing Cycle



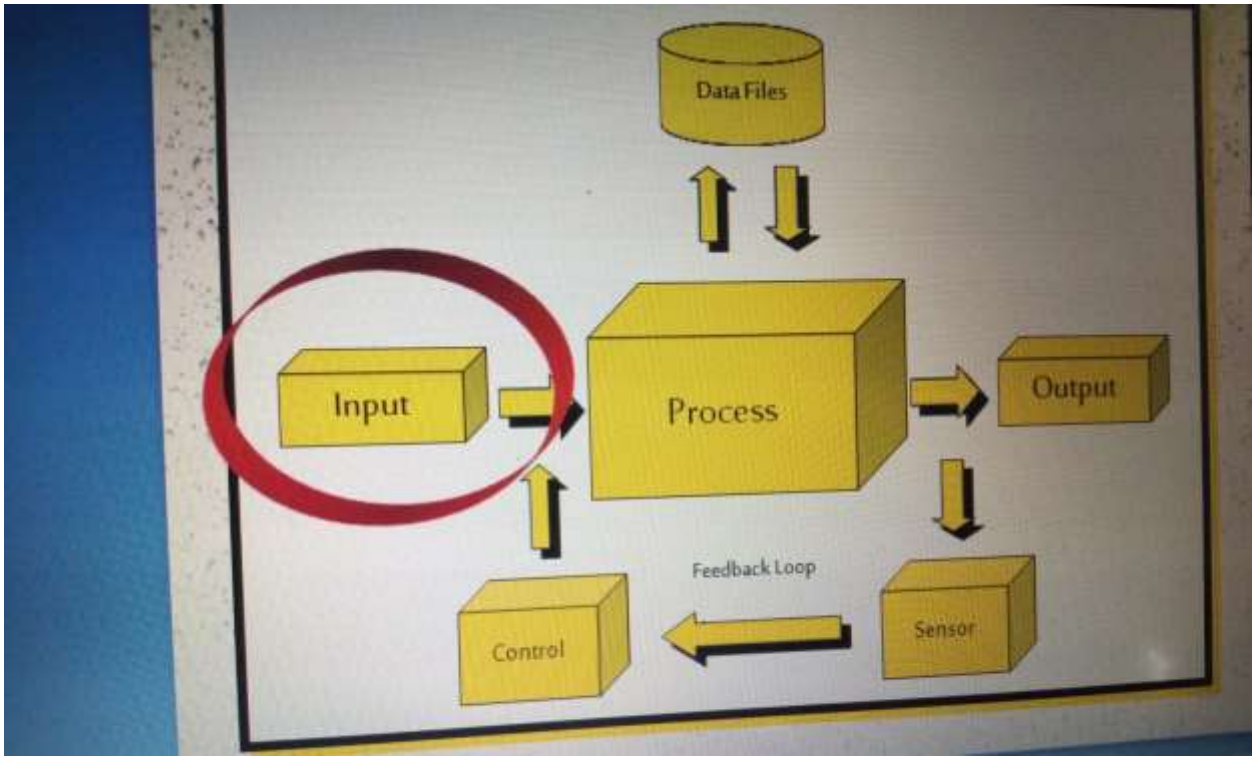
Data Processing Cycle

The resources affected by that event.

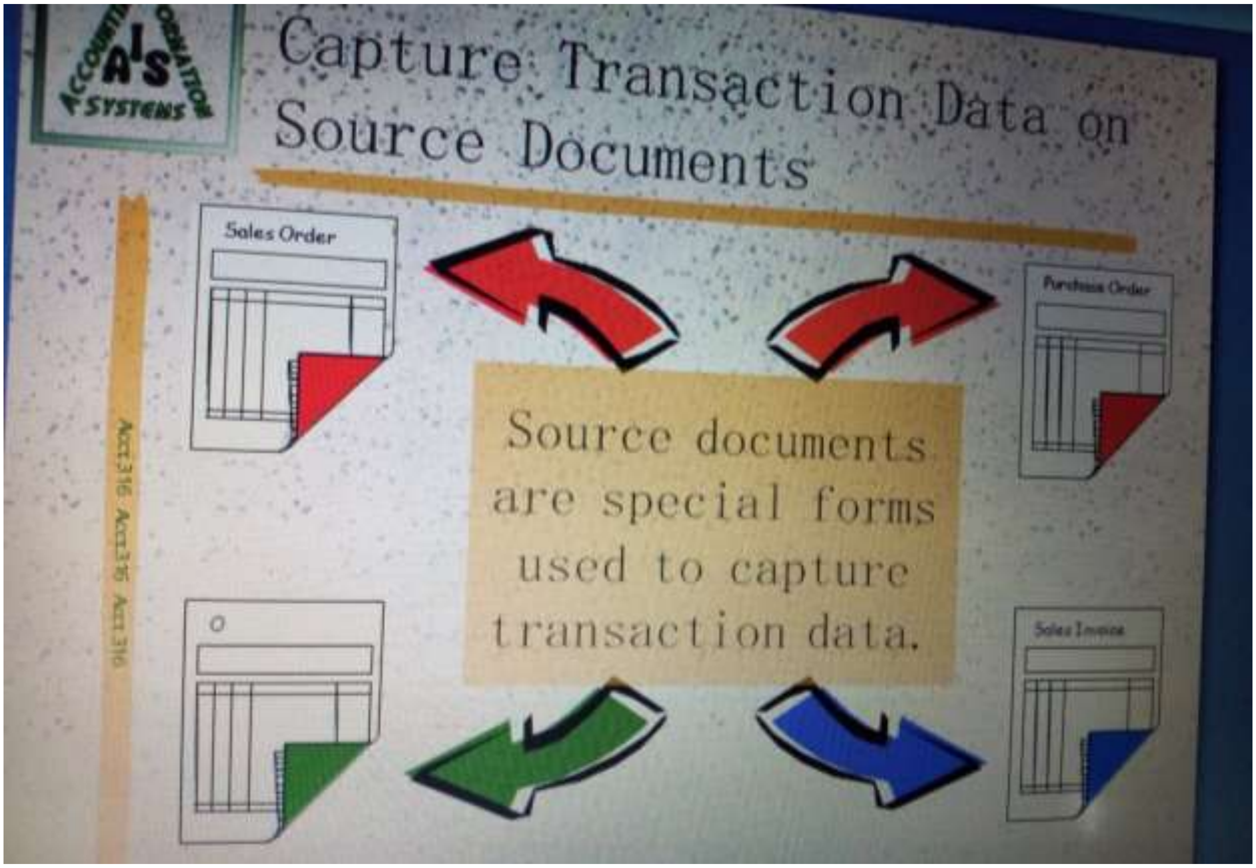
The agents who participate in that event.

e 2-2 Facets of business activites abou ch data must be collected

The Event of Interest



Capture Transaction Data on Source Documents

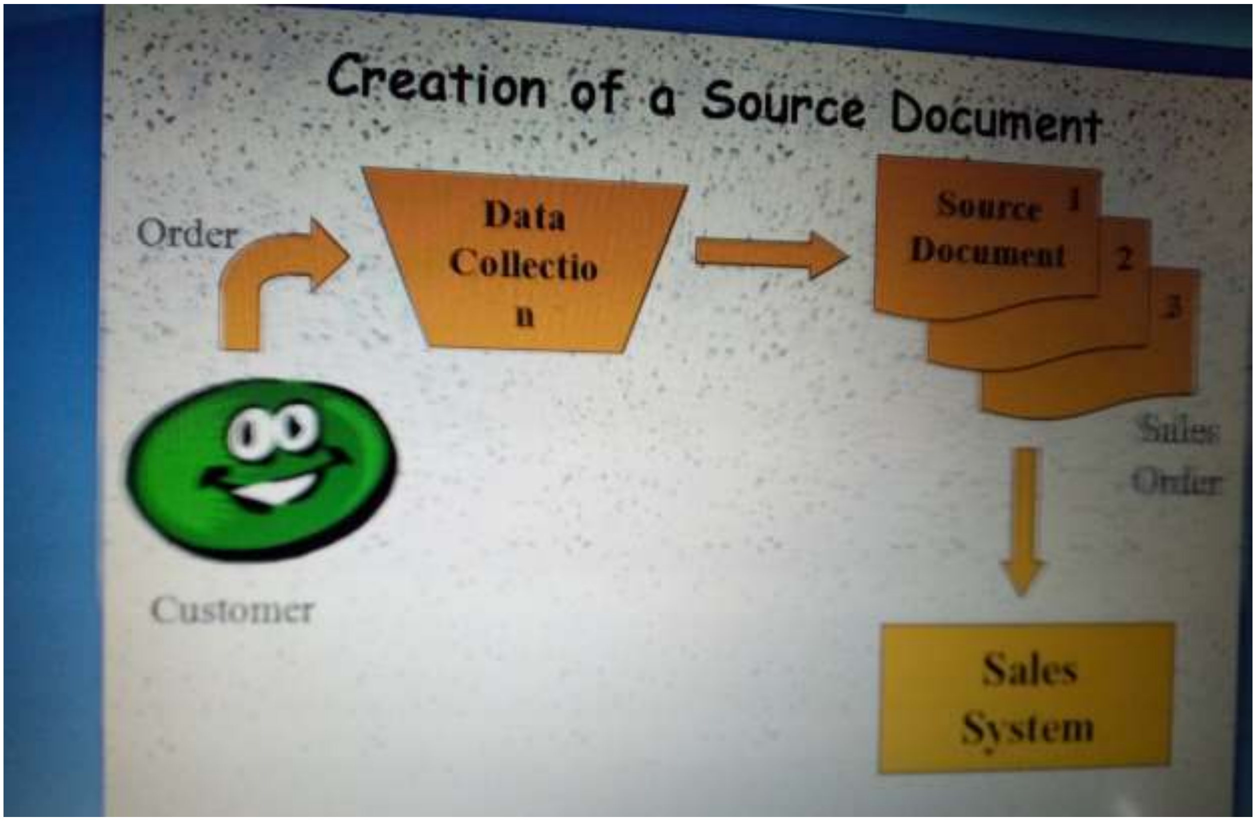

Accounting Information Systems
AIS
Sales Order
Purchase Order
Sales Invoice
Acct 316 Acct 316 Acct 316

Capture Transaction Data on Source Documents

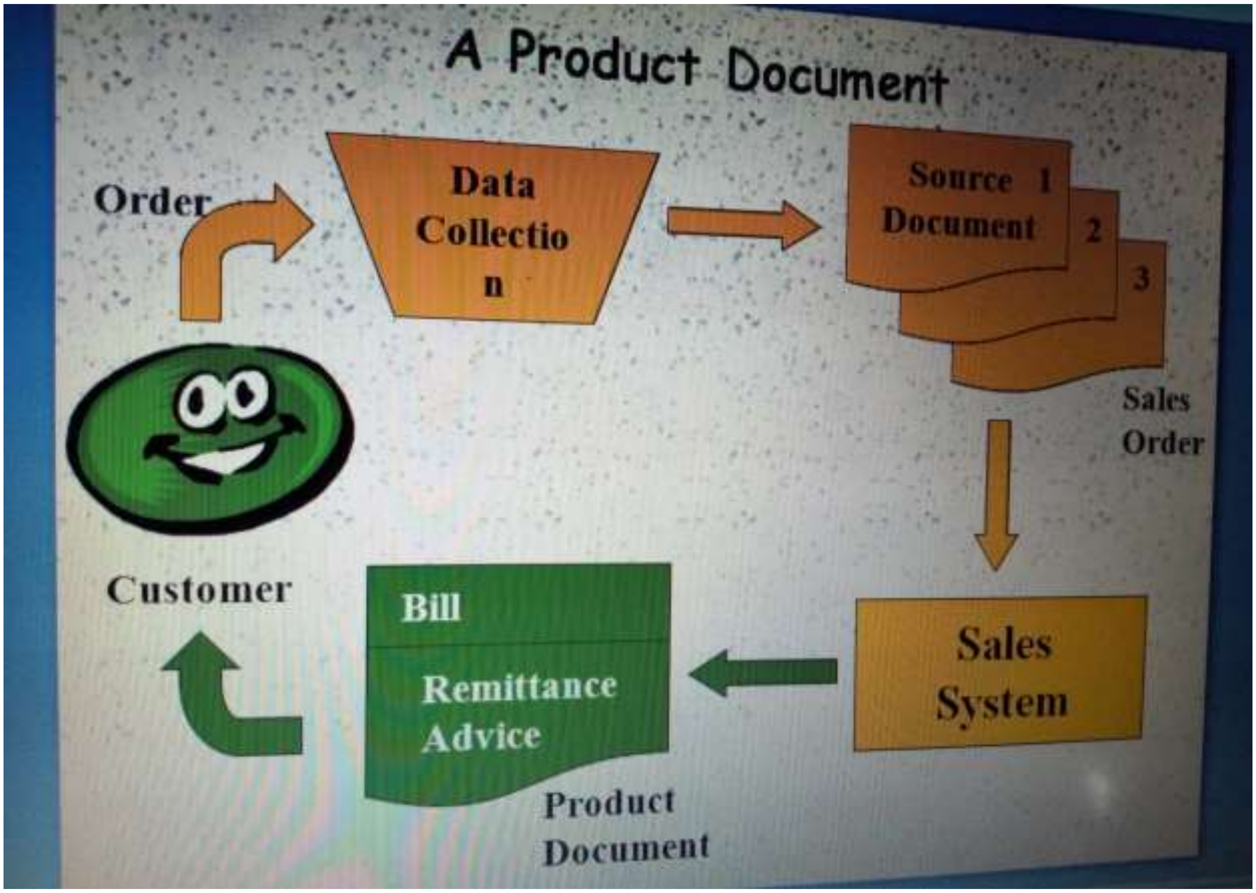
Source documents are special forms used to capture transaction data.

- Control over data collection is improved by pre-numbering each source document.
- Accuracy and efficiency in recording transaction data can be further improved if source documents are properly designed.
- Input documents can be categorized into three types . . .
  - Source Documents
  - Product Documents
  - Turn-around Documents

Creation of a Source Document



A product document



A Product Document

Order

Data Collectio n

Source Document 1

2

3

Sales Order

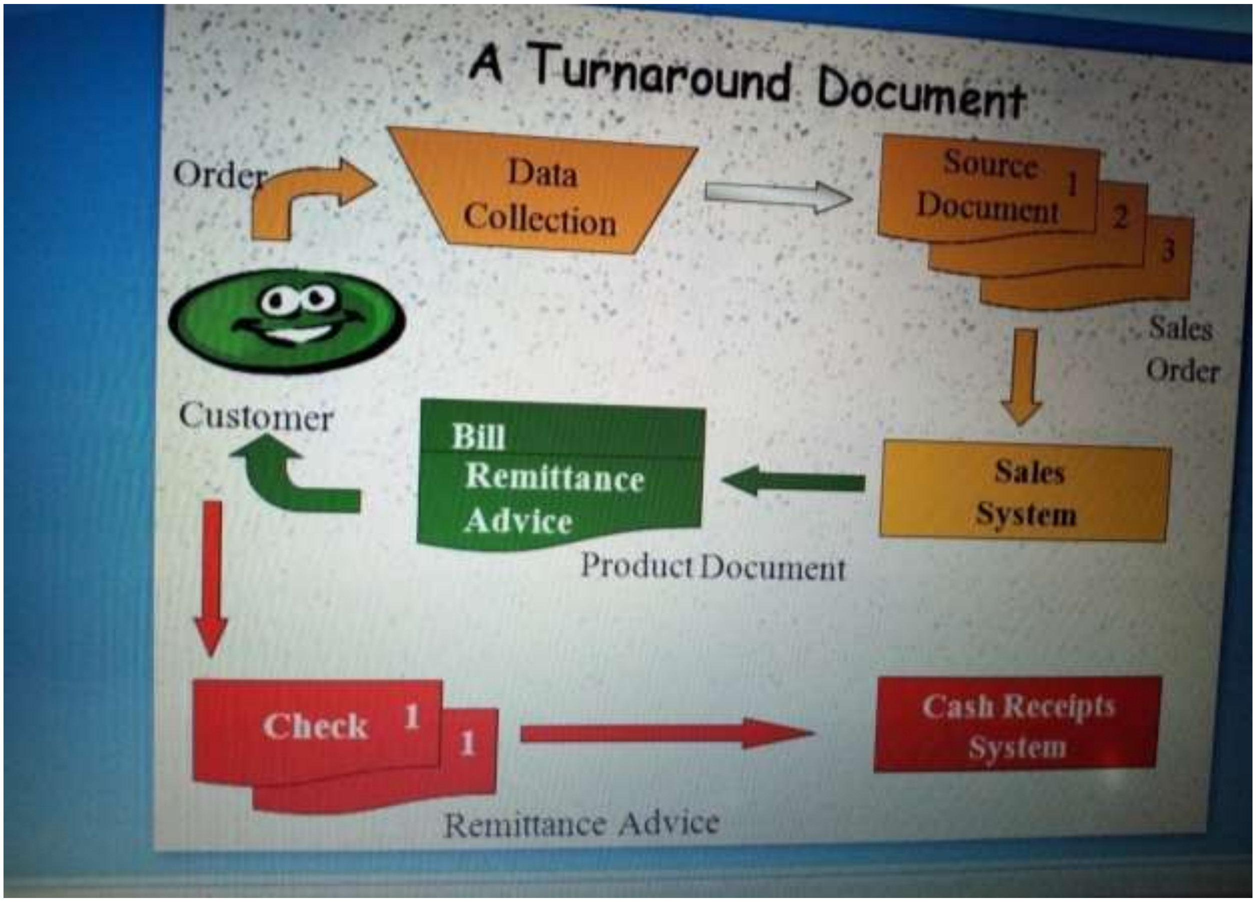
Sales System

Bill

Remittance Advice

Product Document

Customer



A Turnaround Document

3.5 Common Source Documents & Functions

a. Expenditure Cycle

Source Document	Function
Sales Order	Record Customer Order
Delivery Ticket	Record Delivery to Customer
Remittance Advice	Receive Cash
Deposit Slip	Record Amounts Deposited
Credit Memo	Support Adjustments to Customer Accounts

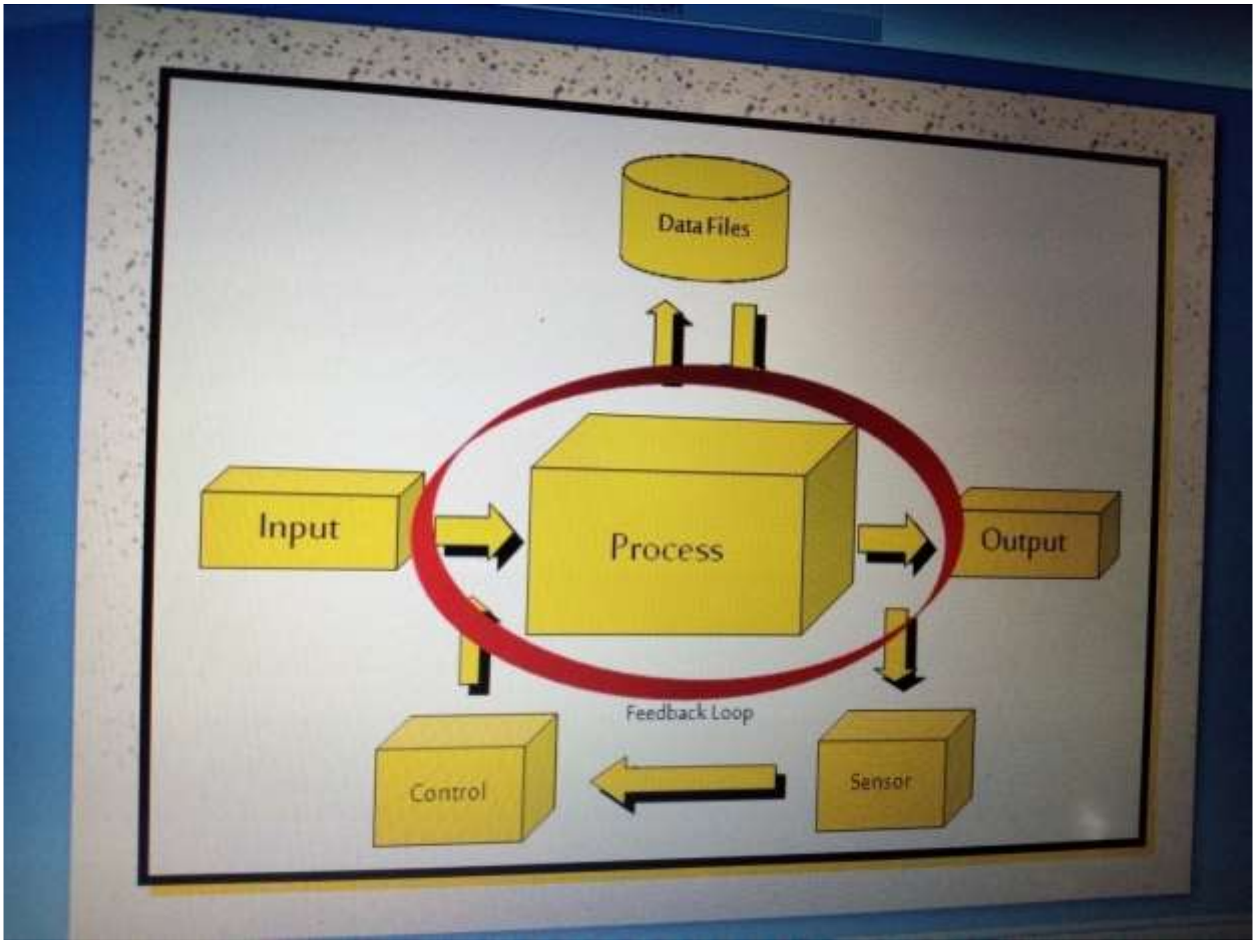
b. Human Resource

Source Document	Function
W4 forms	Collect employee withholding data.
Time cards	Record time worked by employees.
Job time tickets	Record time spent on specific jobs.

c. General Ledger & Reporting System

Source Document	**Function**

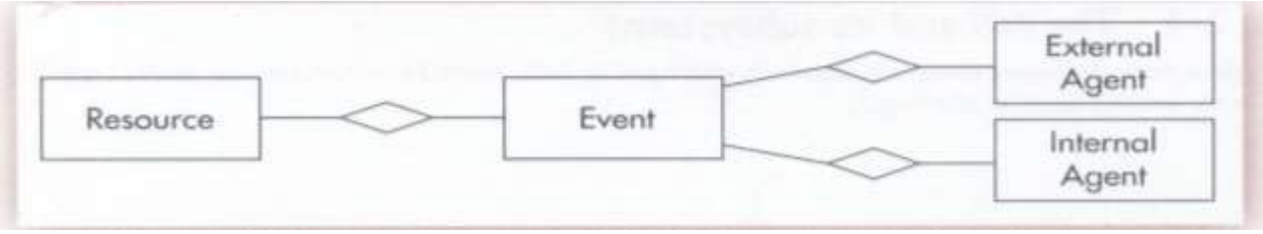
Journal Voucher	Record entry posted to general ledger.



3.5.1 Data Processing

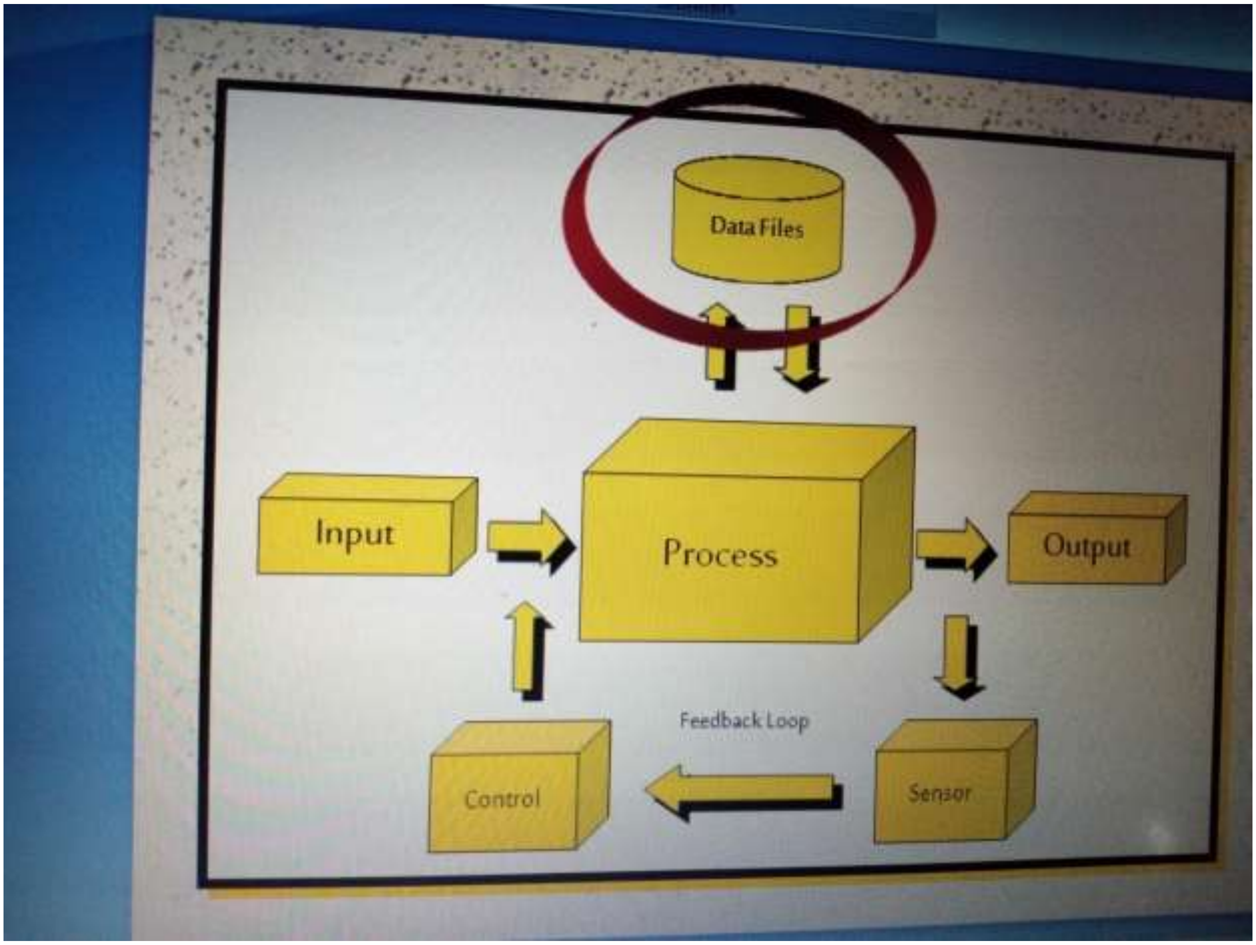
Updating previously stored information about the resources affected by the event and agents who participated in the activity.

Facets of business activities about which data must be collected



- Periodic updating of the data stored is referred to as **batch processing**.
- Immediate updating as each transaction occurs is referred to as **on-line, real-time processing**.

Note: Audit Trail - An audit trail provides a means to check the accuracy and validity of ledger postings.

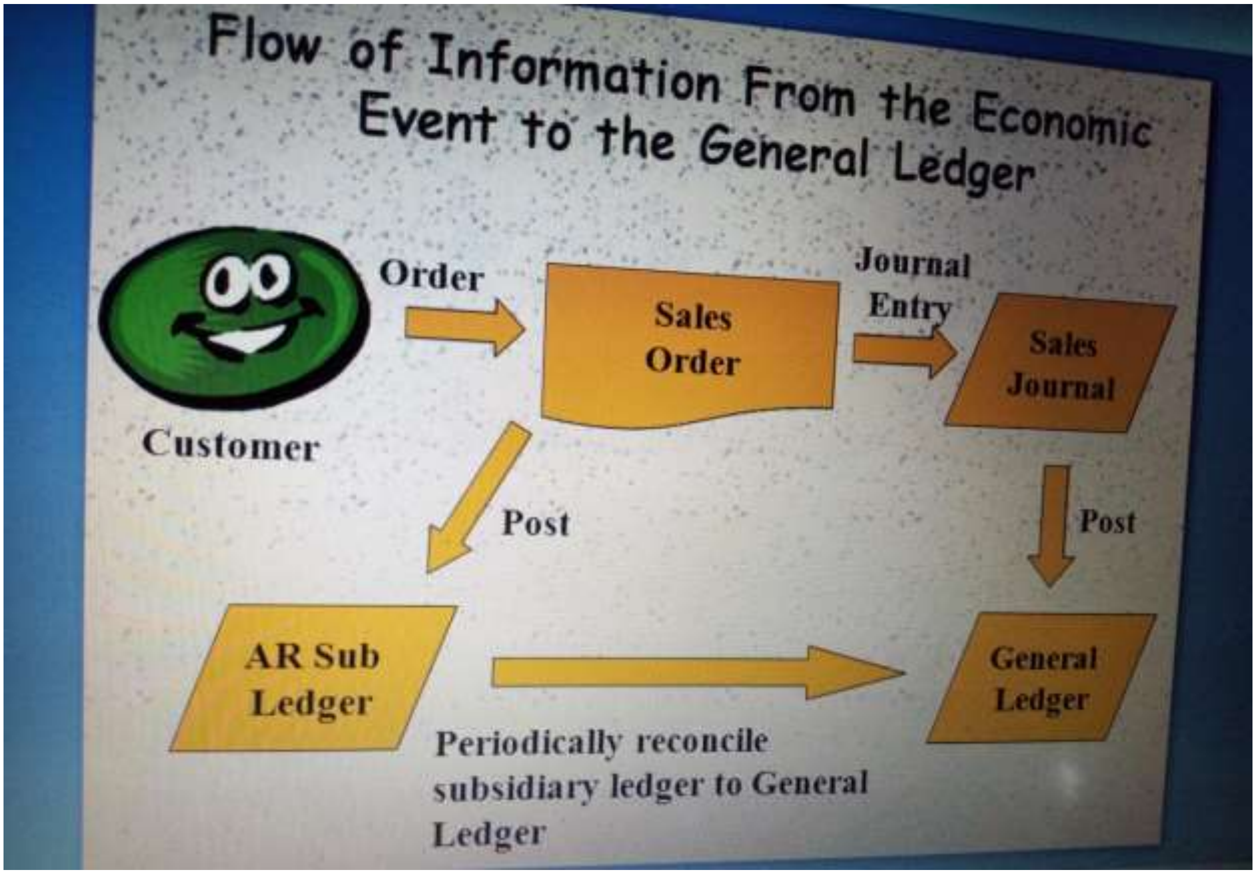


Storage . . .

Ledgers and files provide storage of data in both manual and computerized systems.

- The General Ledger
- The Accounts Payable Ledger
- The Accounts Receivable Ledger

A **ledger** is . . .a book of financial accounts, which reflect the financial effects of the firm's transactions after they are posted from the various journals.



Flow of Information From the Economic Event to the General Ledger

Customer

Order

Sales Order

Journal Entry

Sales Journal

Post

Post

AR Sub Ledger

General Ledger

Periodically reconcile subsidiary ledger to General Ledger

A **file** is an organized collection of data.

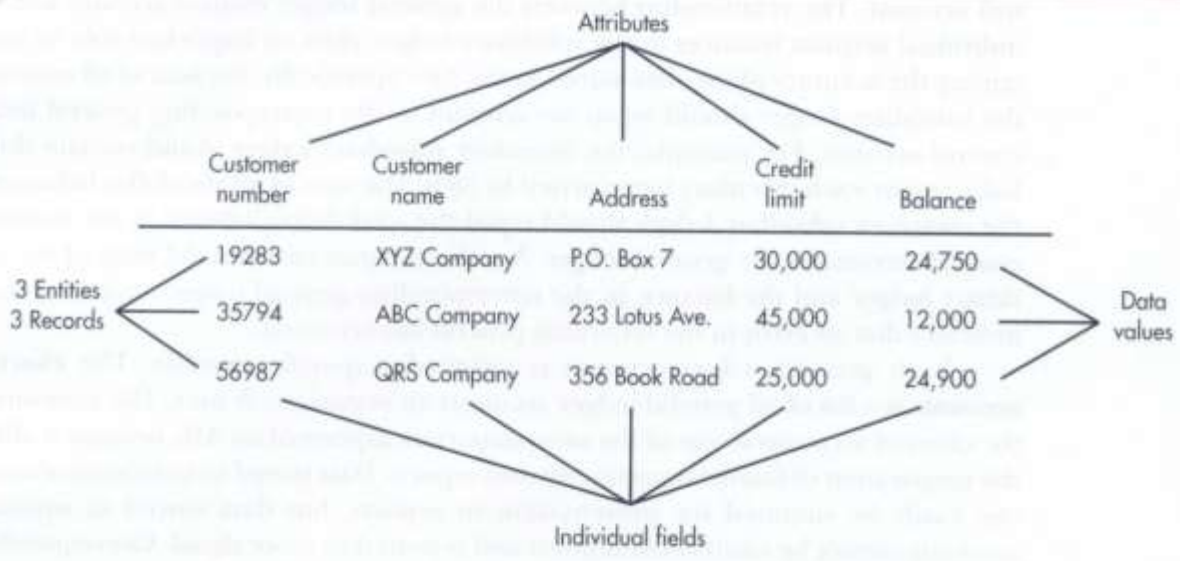
Files may be

- Manual
- Computer (magnetic)

A **transaction file** is a collection of transaction input data - normally **temporary** in nature.

A master file is - a collection of data that are of a more permanent or continuing interest.

Data storage elements – *Figure Below*



This accounts receivable file stores information about three separate entities: XYZ Company, ABC Company, and QRS Company. As a result, there are three records in the file. Five separate attributes are used to describe each customer: customer number, customer name, address, credit limit, and balance. There are therefore five separate fields in each record. Each field contains a data value that describes an attribute of a particular entity (customer). For example, the data value 19283 is the customer number for the XYZ Company.

3.5.2 AIS Function #2

A. To provide management with information useful for decision making.
   This information is provided in the form of reports that fall into two main categories:
   i. Financial Statements
   ii. Managerial Reports
B. Provide adequate controls to ensure that data are recorded and processed accurately.
C. Ensure that the information produced by the system is reliable.
D. Safeguard organizational assets.
E. Ensure that business activities are performed efficiently and in accordance with management's objectives.

3.6 Internal Control Considerations

What are two important methods for accomplishing these objectives?

i. Provide for adequate documentation of all business activities.

ii. Design the AIS for effective segregation of duties.

i. Adequate Documentation

Documentation allows management to verify that assigned responsibilities were completed correctly**.**

What is Segregation of Duties?

……..Segregation of duties refers to dividing responsibility for different portions of a transaction among several people.

What functions should be performed by different people?

- Authorizing transactions
- Recording transactions
- Maintaining custody of assets

Types of Internal Controls

- Taking preventive measures
- Detecting errors or when fraud may take place
- Correcting the mess before it takes place

Summary of the study

In this study we have covered the following:
Production cycle, human resources, payroll
General ledger and reporting

Questions for the class

1. Discuss in brief the origin of E-business.
2. What are the advantages and disadvantages of E-Business?
3. What are the prerequisites of E-business procedure?
4. What are the major differences between E-business and E-commerce? What is an Enterprise Resource Planning or ERP?
5. Discuss a business transaction in detail.

Unit 4

4.0 SYSTEMS DESIGN, IMPLEMENTATION AND OPERATION

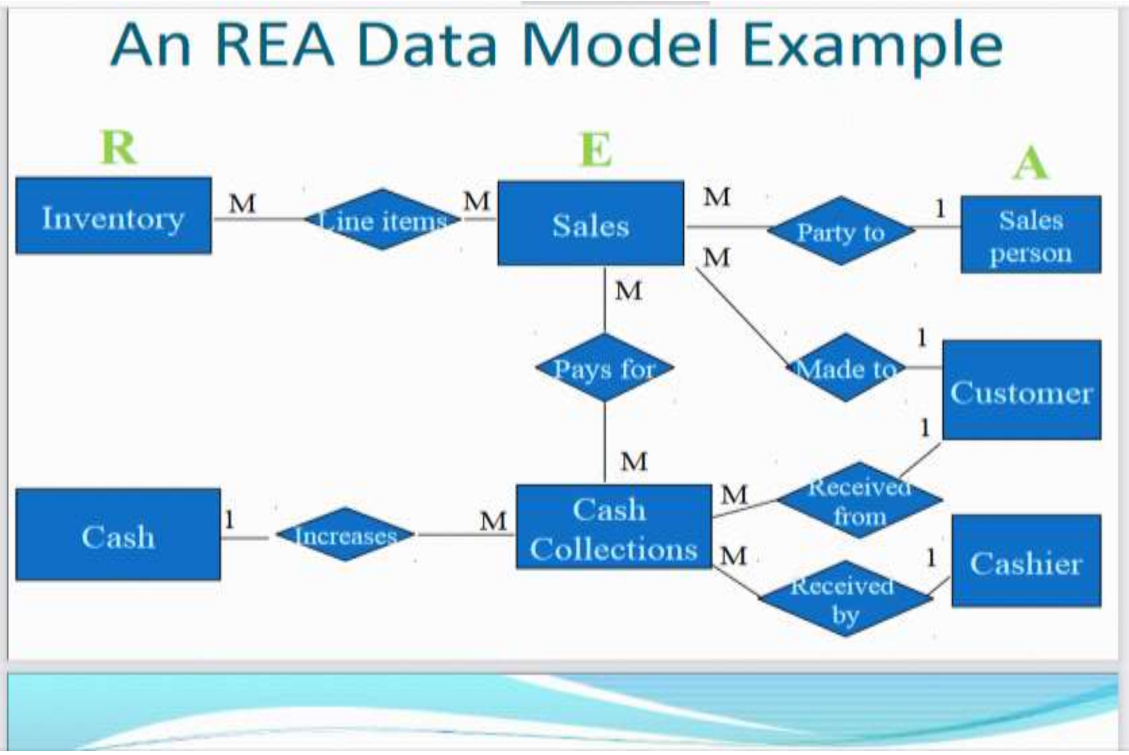
Unit study Objectives

At the end of the study the students should be able to:

1. Learn on how to design an AIS
2. How the AIS is implemented
3. Learn how REA data model can be used to design an AIS database. How an entity-relationship (E-R) diagram of an AIS database drawn. How the E-R diagrams read, and what they reveal about the business activities and policies of the organization being modeled.

4.1 Database Design Using the REA Data Model

The diagram of REA Data Model



An REA Data Model Example

4.2 Introduction

Steps in database design include the following:

1. Planning

Initial planning to determine the need for and feasibility of developing a new system. Includes preliminary judgments about technological and economic feasibility.

2. Requirements analysis

Identifying user information needs. Defining scope of proposed system. Using information about the expected number of users and transaction volume to make preliminary decisions on hardware and software requirements.

3. Design

Developing different schemas for the new system at the conceptual, external, and internal levels.

4. Coding

Translating the internal-level schema into the actual database structures that will be implemented in the new system. Developing new applications.

5. Implementation

Transferring data from existing systems to the new database. Testing the new system. Training employees.

6. Operation and maintenance

Using and maintaining the new system. Monitoring system performance and user satisfaction to determine need for enhancements and modifications.

Eventually, changes in business strategy and practices or new IT developments lead to the need for a new system and the process starts over.

Accountants can and should participate in all stages of the database design process, although participation varies between stages.

- Planning stage

Accountants provide information to help evaluate feasibility. Participate in the feasibility decision.

- Requirements analysis and design stages

Accountants participate in Identifying user needs, Developing logical schemas, Designing data dictionary and Specifying controls.

- Coding stage

Accountants with good AIS skills may participate in coding.

- Implementation stage

Accountants help test accuracy of database and application programs

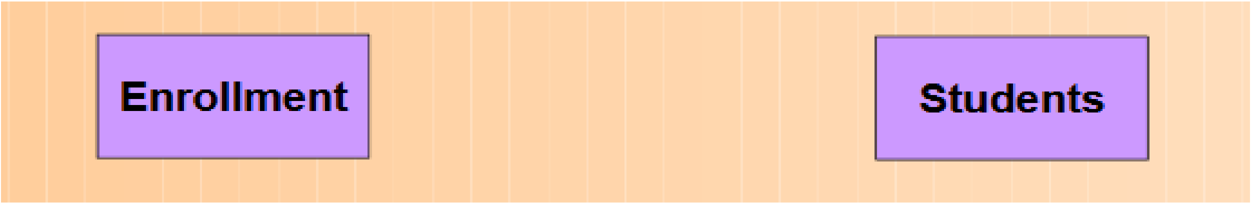
- Operation and maintenance stage

Accountants use the database system to process transactions. Sometimes help manage it.

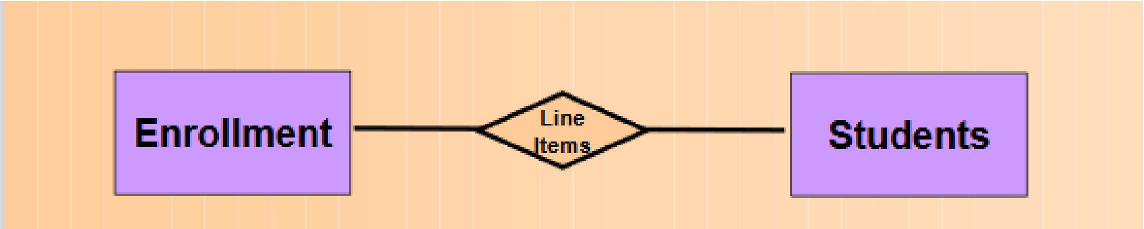
Accountants may provide the greatest value by taking responsibility for *data modeling*—the process of defining a database to faithfully represent all aspects of the organization, including interactions with the external environment. Occurs during both requirements analysis and design stage. Two important tools to facilitate data modeling:

i. ***Entity-relationship diagramming***

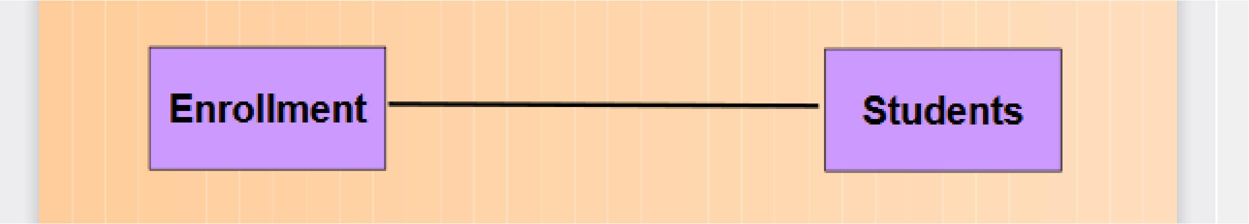
An entity-relationship (E-R) diagram is a graphical technique for portraying a database schema. Shows the various entities being modeled and the important relationships among them. In an E-R diagram, entities are depicted as rectangles. But there are no industry standards for other aspects of these diagrams.



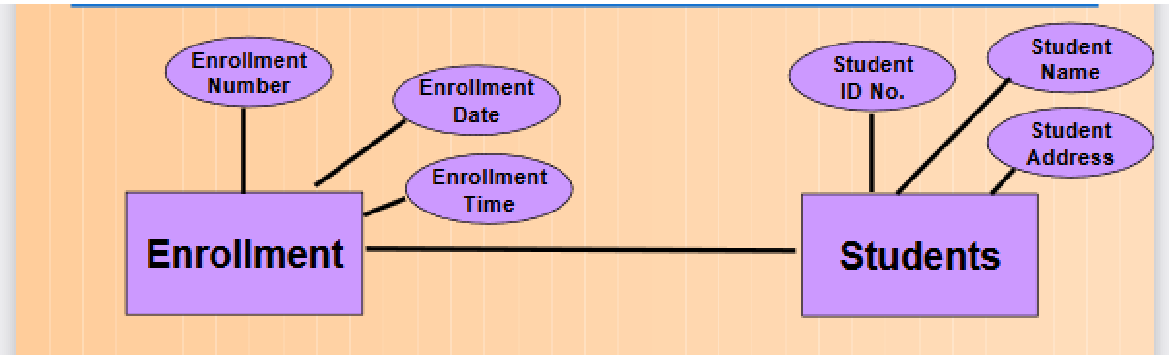
Some data modelers, tools, and authors use diamonds to depict relationships.



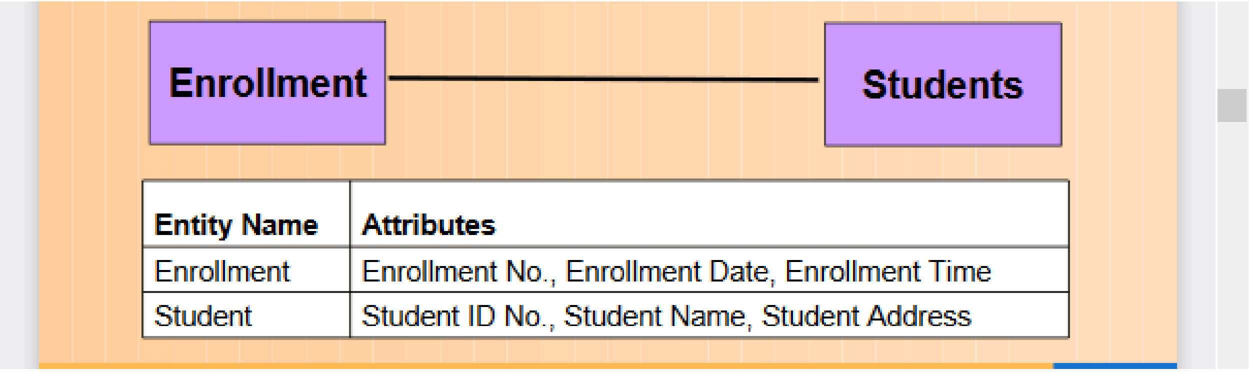
Others do not use diamonds.



Sometimes the attributes associated with each entity are depicted as named ovals connected to each rectangle



Sometimes these attributes are listed in a separate table.



Entity Name	Attributes
Enrollment	Enrollment No., Enrollment Date, Enrollment Time
Student	Student ID No., Student Name, Student Address

In this unit study, we will create E-R diagrams with a large number of entities and relationships. To reduce clutter and improve readability, we omit diamonds and list attributes in a separate table.

E-R diagrams can be used to represent the contents of any kind of databases. Our focus is on databases designed to support an organization's business activities. The diagrams we develop depict the contents of a database and graphically model those business processes.

In addition to their use in designing databases, E-R diagrams can be used to:

- Document and understand existing databases.
- Re-engineer business processes.

In this chapter, we'll use E-R diagrams for designing new databases and understanding existing ones.

E-R diagrams can include many different kinds of entities and relationships. An important step in designing a database is deciding which entities need to be modeled. The REA data model is useful for this decision.

ii. ***REA DATA MODEL***

The REA data model was developed specifically for use in designing accounting information systems.

- Focuses on business semantics underlying an organization's value chain activities.
- Provides guidance for:
  - Identifying the entities to be included in a database.
  - Structuring the relationships among the entities.

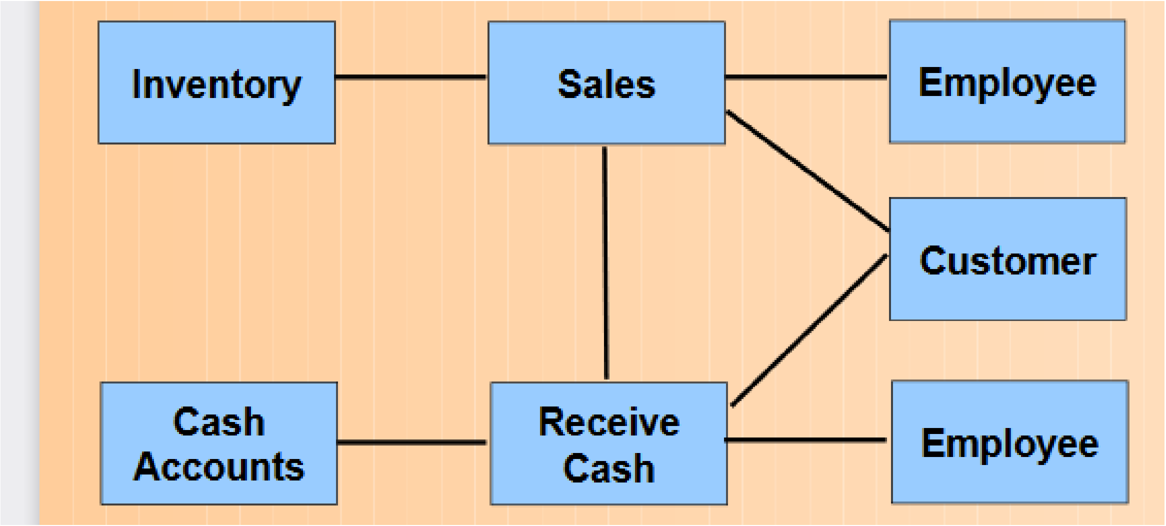
REA data models are usually depicted in the form of E-R diagrams.

Therefore, we refer to E-R diagrams developed with the REA model as REA diagrams.

Three Basic Types of Entities

- The REA data model is so named because it classifies entities into three distinct categories:
  a. ***Resources*** that the organization acquires and uses. [Resources are things that have economic value to the organization].
  b. ***Events*** in which the organization engages [These are the various business activities about which management wants to collect information for planning or control purposes].
  c. ***Agents*** participating in these events [Includes people and organizations who participate in events and about whom information is desired for planning, control, and evaluation purposes].

*Can you identify the **Resources, Events and Agents** in this diagram below?*

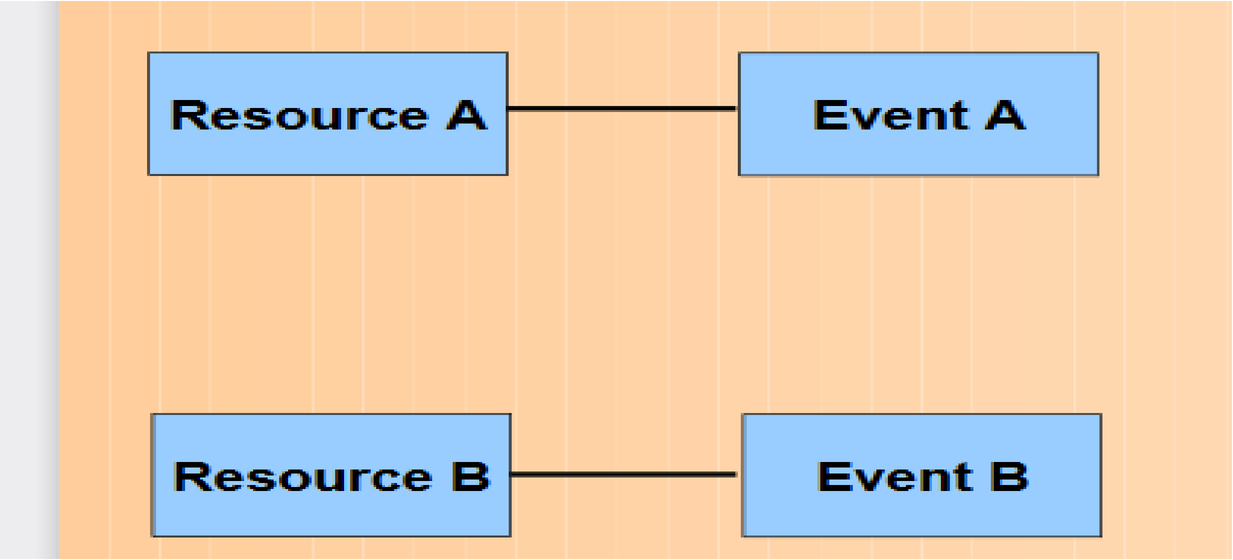


Answer: ***Inventory and Cash Accounts*** are the ***Resource***, while ***Sales* and *Receive Cash*** are ***Events*** and lastly ***Employee, Customer, employee*** are the ***Agents.***

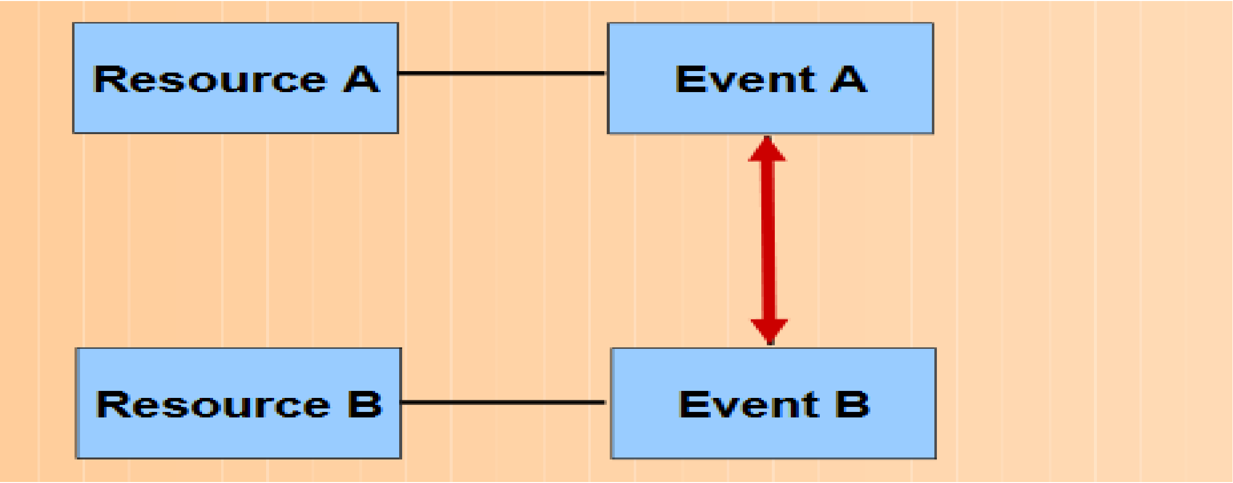
Structuring Relationships: The Basic REA Template

The REA data model prescribes a basic pattern for how the three types of entities (resources, events, and agents) should relate to one another.

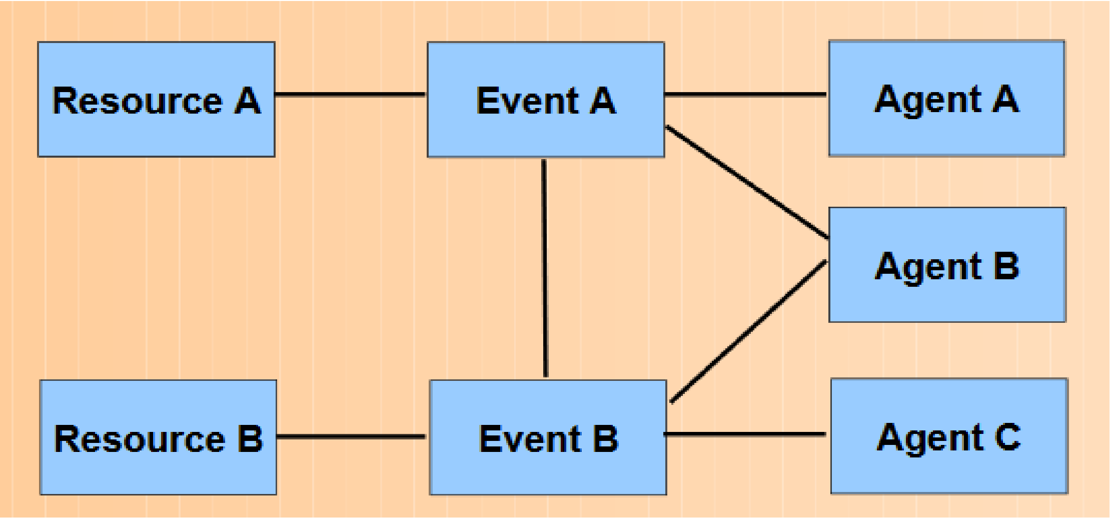
a. Rule 1: Each event is linked to at least one resource that it affects.



b. Rule 2: Each event is linked to at least one other event.



c. Rule 3: Each event is linked to at least two agents



Let's take a closer look at each of these three rules

Rule 1: *Every event entity must be linked to at least one resource entity*

- Events must be linked to at least one resource that they affect.
  - Some events affect the quantity of a resource:
    - If they increase the quantity of a resource, they are called a "get" event.
    - If they decrease the quantity of a resource they are called a "give" event.
    - EXAMPLE: If you purchase inventory for cash:
      » The get event is that you receive inventory.
      » The give event is that you pay cash.
    - Relationships that affect the quantity of a resource are sometimes referred to as *stockflow* relationships.

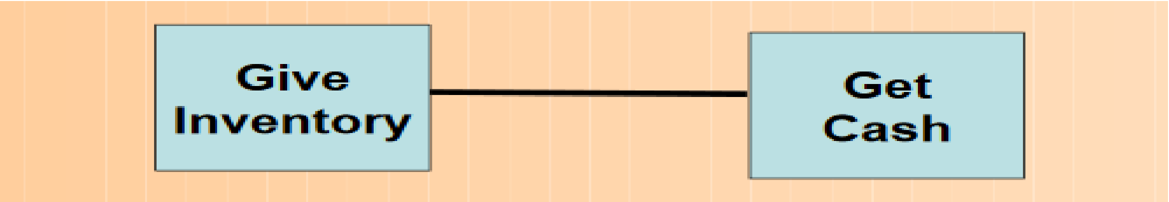
Not every event directly alters the quantity of a resource. If a customer orders goods but has not paid and has not received goods, this activity is called a commitment event.

- Organizations track the effects of commitments to provide better service and for planning purposes.

Rule 2: Every event entity must be linked to at least one other event entity

- Give and get events are linked together in what is labeled an economic duality relationship. These relationships reflect the basic business principle that organizations engage in activities that use up resources in hopes of acquiring other resources in exchange. Each accounting cycle can be described in terms of give-to-get economic duality relationships.

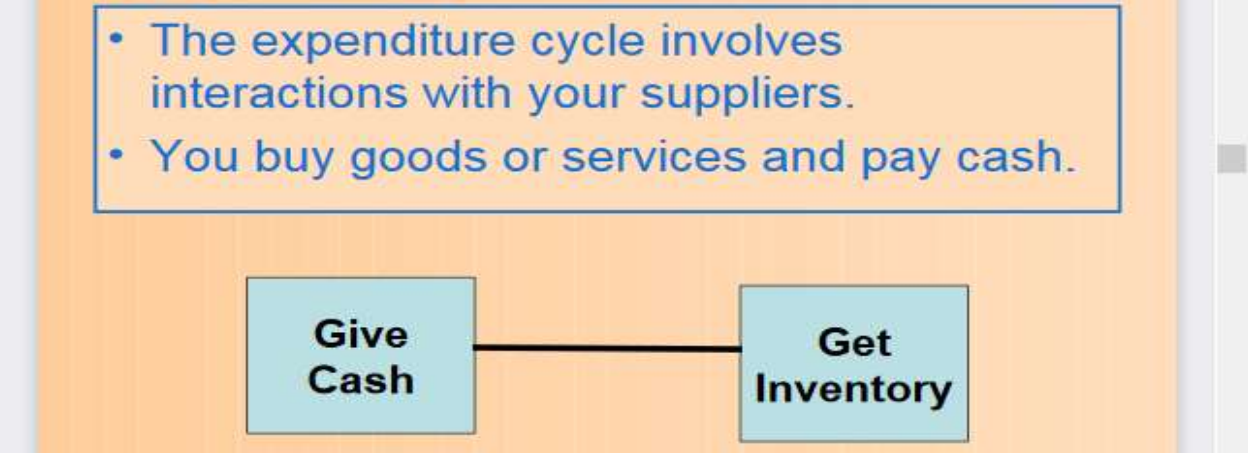
The revenue cycle involves interactions with your customers. You sell goods or services and get cash.



Give Inventory

Get Cash

The expenditure cycle involves interactions with your suppliers. You buy goods or services and pay cash.

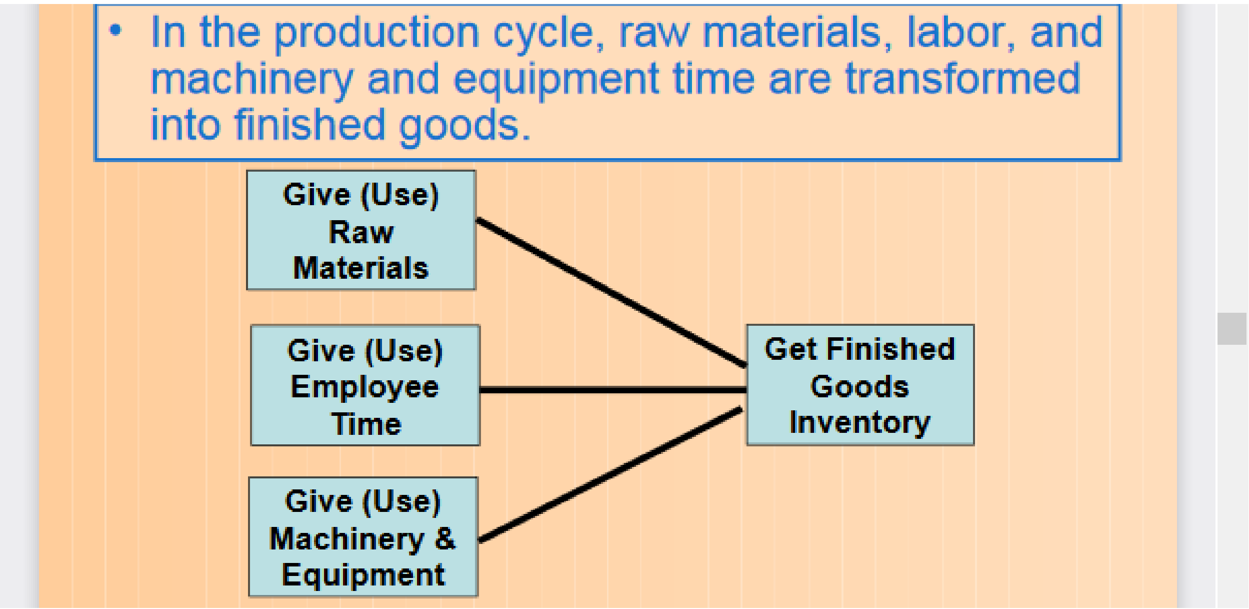


- The expenditure cycle involves interactions with your suppliers.
- You buy goods or services and pay cash.

Give Cash

Get Inventory

In the production cycle, raw materials, labor, and machinery and equipment time are transformed into finished goods.



- In the production cycle, raw materials, labor, and machinery and equipment time are transformed into finished goods.

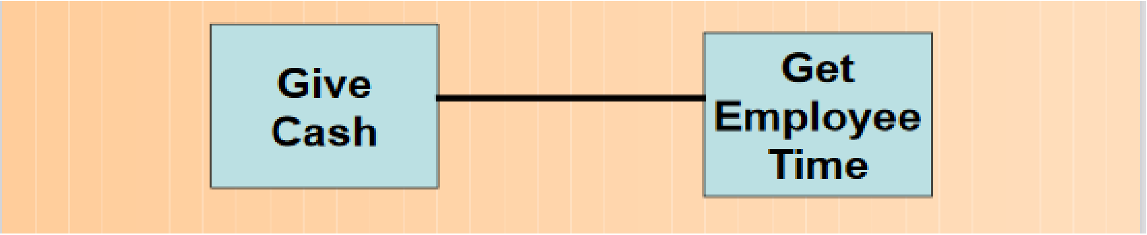
Give (Use) Raw Materials

Give (Use) Employee Time

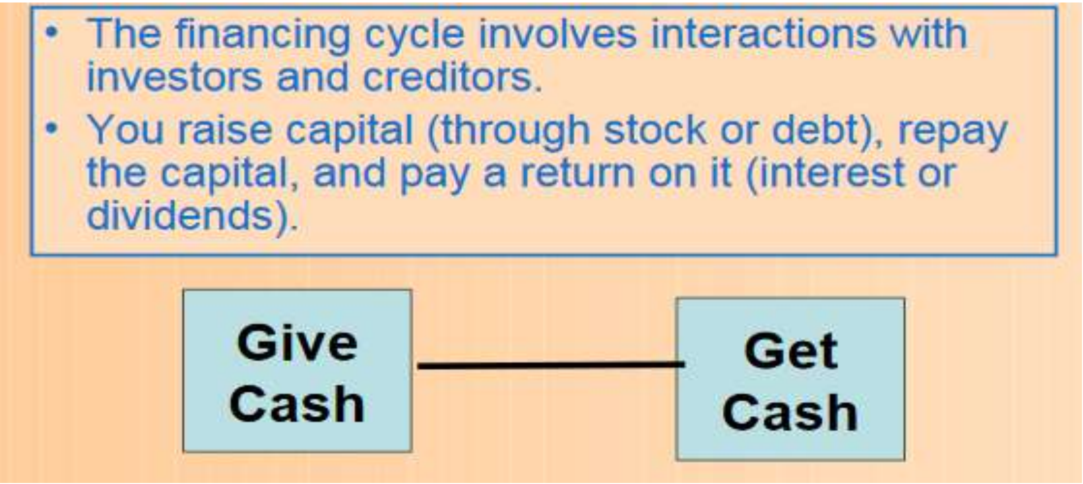
Give (Use) Machinery & Equipment

Get Finished Goods Inventory

The human resources cycle involves interactions with your employees. Employees are hired, trained, paid, evaluated, promoted, and terminated.



The financing cycle involves interactions with investors and creditors. You raise capital (through stock or debt), repay the capital, and pay a return on it (interest or dividends).



- The financing cycle involves interactions with investors and creditors.
- You raise capital (through stock or debt), repay the capital, and pay a return on it (interest or dividends).

Not every relationship between two events represents a give-to-get economic duality.

- Commitment events are linked to other events to reflect sequential cause-effect relationships. *Example*: Take customer order (commitment) leads to: Deliver inventory (give event) and receive cash (get event).

Rule 3: Every event entity must be linked to at least two participating agents

- For accountability, organizations need to be able to track actions of employees.
- Also need to monitor the status of commitments and exchanges with outside parties.
- Each event links to at least two participating agents.

For events that involve transactions with external parties:

- The internal agent is the employee responsible for the affected resource.
- The external agent is the outside party to the transaction.

For internal events, such as transferring raw materials to the production floor:

- The internal agent is the employee who gives up responsibility or custody for the resource.
- The external agent is the one who receives it.

To design an REA diagram for an entire AIS, one would develop a model for each transaction cycle and then integrate the separate diagrams into an enterprise-wide model. In this chapter, we focus on the individual transaction cycles.

Developing an REA diagram for a specific transaction cycle consists of three steps:

- STEP ONE: Identify the events about which management wants to collect information.
- STEP TWO: Identify the resources affected by the events and the agents who participated.
- STEP THREE: Determine the cardinalities between the relationships.

Let's walk through an example, starting with step one.

STEP ONE: IDENTIFY RELEVANT EVENTS

- At a minimum, every REA model must include the two events that represent the basic give-to-get" economic exchange performed in that transaction cycle.
- The give event reduces one of the organization's resources.
- The get event increases a resource.
- There are usually other events that management is interested in planning, controlling, and monitoring. These should be included in the model.

Example: Typical activities in the revenue cycle include:

- Take customer order - *Taking the customer order does not involve giving or taking a resource. It is a commitment event*
- Fill customer order - *Filling the order involves a reduction in the company's inventory. It is a give event*
- Bill customer - *Billing customers involves the exchange of information with an external party but does not affect resources.*
- Collect payment - *Collecting payment results in an increase in cash. It is a get event.*

Take customer order	The give-to-get, then, is:
Fill customer order	Fill customer order (often referred to as "sale");
Bill customer	
Collect payment	Collect cash (often referred to as "cash receipt").

Take customer order	**Should "take customer order" and "bill customer" be included in the model?**
Fill customer order	
Bill customer	
Collect payment	

Take customer order	• Taking an order requires that we set resources aside.

Fill customer order	• That information should be included in our model.
Bill customer	
Collect payment	

Take customer order	• Printing and mailing invoices does not directly affect an economic resource. • It does not represent a commitment on the part of the company to a future exchange. • It is an information retrieval event and should not alter the contents of the database. • Does not need to be included in the model.
Fill customer order	
Bill customer	
Collect payment	

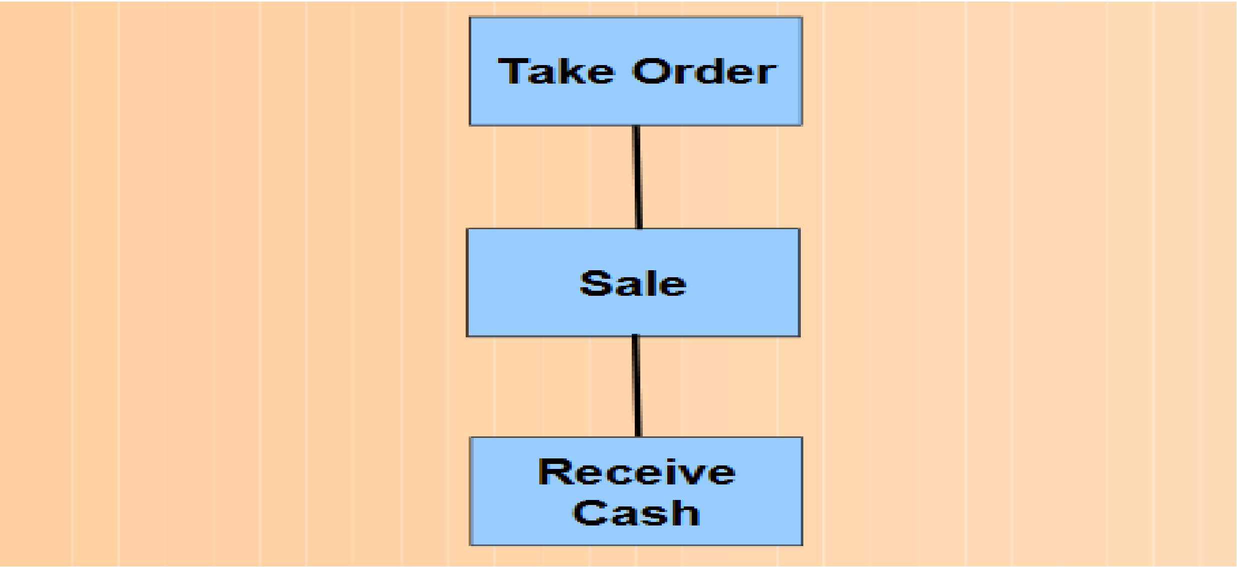
While accounts receivable is an asset in financial reporting, it is not represented as a resource in an REA model.

- It represents the difference between total sales to a customer and total cash collections from the customer.
- The information to calculate an accounts receivable balance is already there because the sales and cash receipt information is captured.

Events that pertain to “entering” data or “re-packaging” data in some way do not appear on the REA model.

- They are not primarily value-chain activities.
- What is modeled is the business event and the facts management wants to collect about the event, not the data entry process.

In completing the first step of an REA diagram, the event entities are typically drawn from top to bottom in the sequence in which they normally occur.

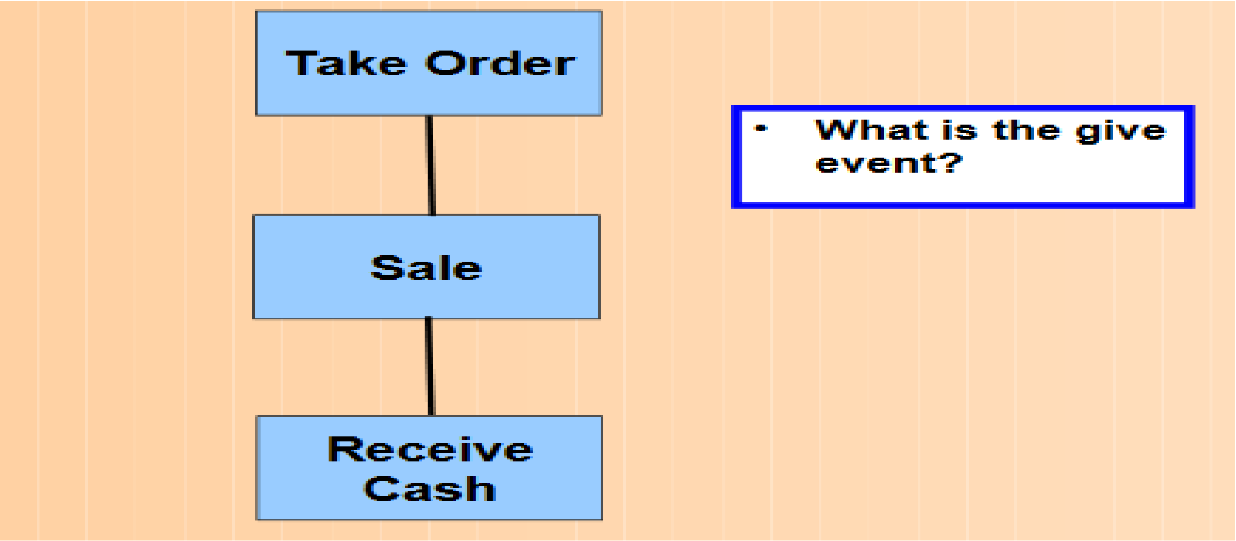


STEP TWO: Identify the resources affected by the events and the agents who participated.

STEP TWO: IDENTIFY RESOURCES AND AGENTS

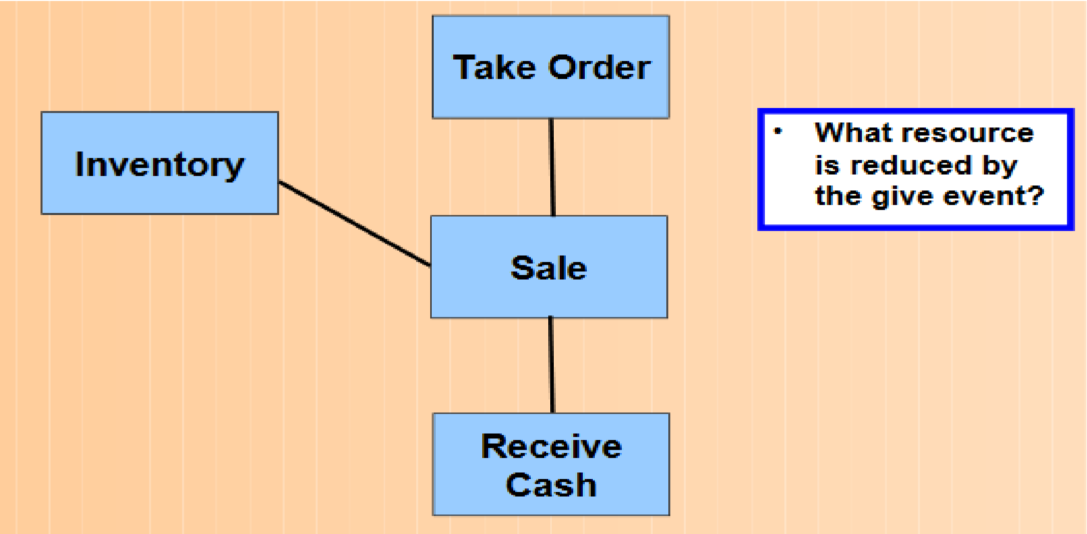
When the relevant events have been diagrammed in the center of the REA diagram, the resources that are affected by those events need to be identified. Involves determining:

- The resource(s) reduced by the give event.
- The resource(s) increased by the get event.
- The resources that are affected by a commitment event.

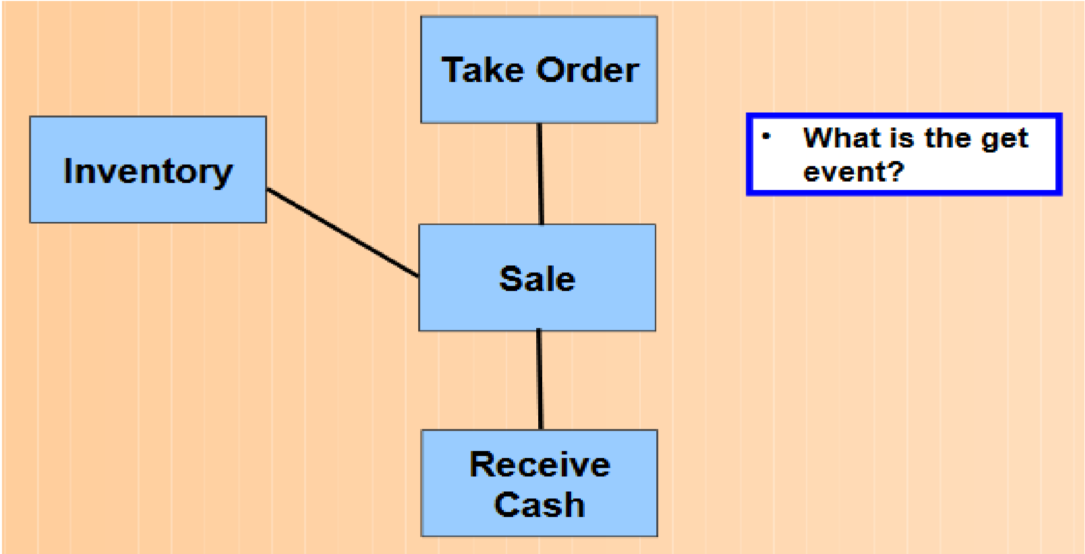


- What is the give event?

Sale is the **Give Event** here in the above table

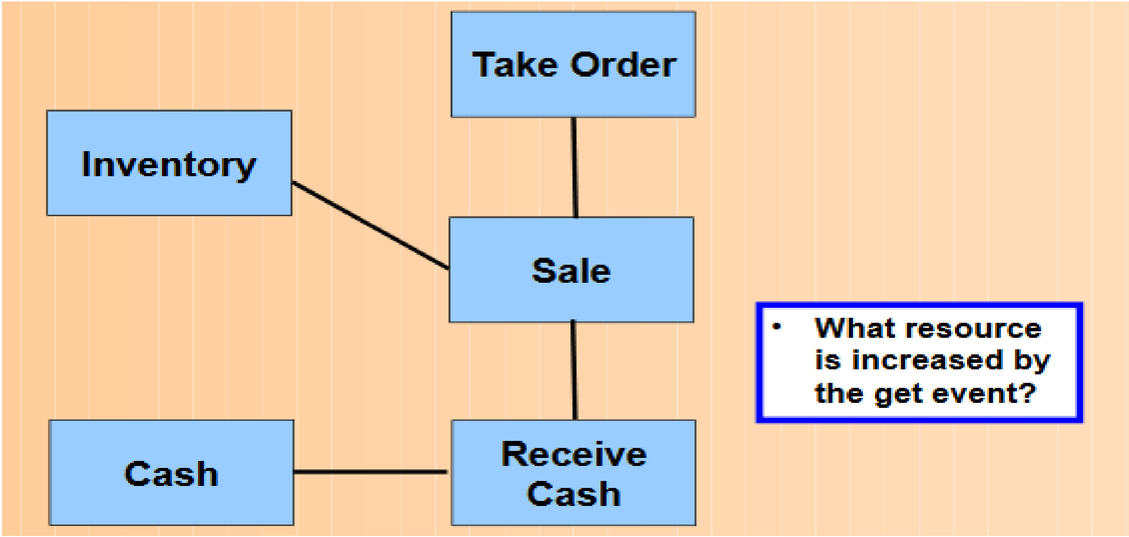


- What resource is reduced by the give event?

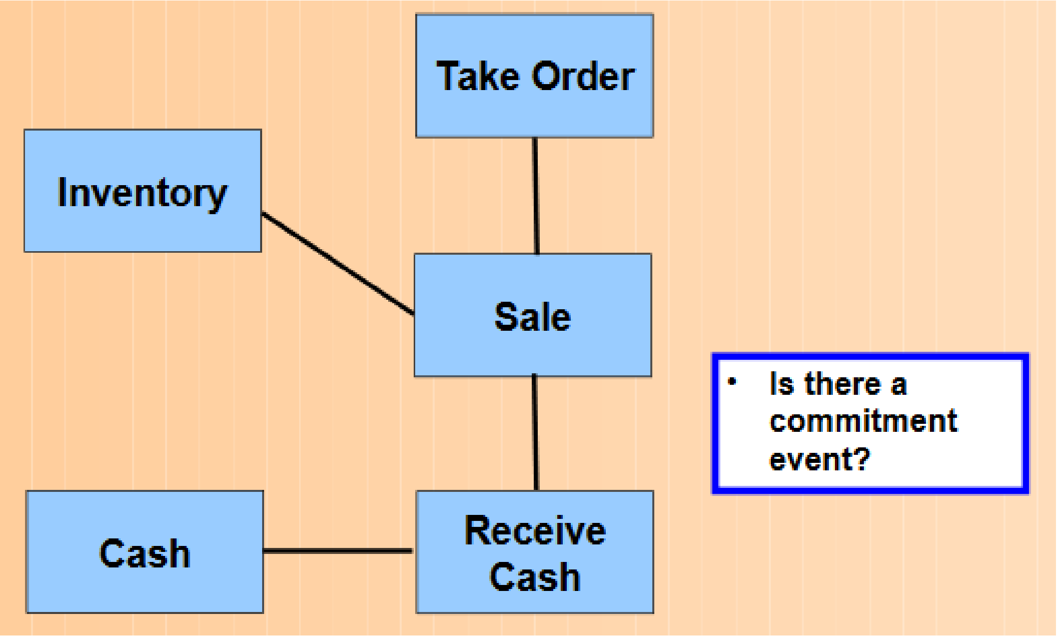


- What is the get event?

The get event here is **Receive Cash** in the above table

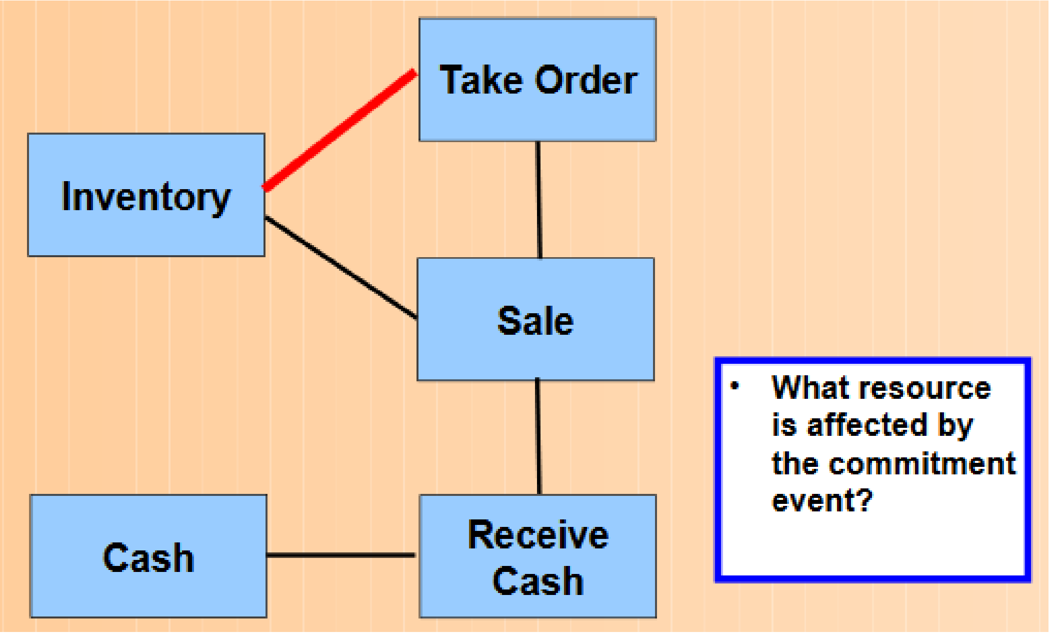


- What resource is increased by the get event?



- Is there a commitment event?

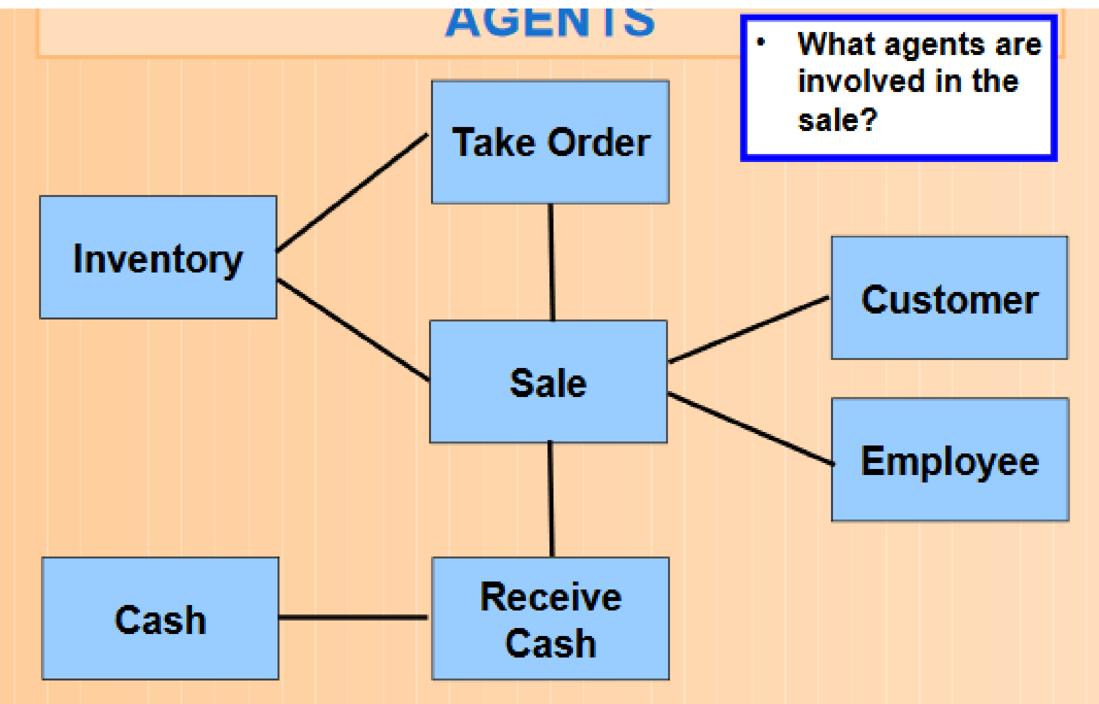
Take Order the commitment event in the above table



- What resource is affected by the commitment event?

The agents who participate in each event should also be identified.

- There will always be at least one internal agent (employee).
- In most cases, there will also be an external agent (e.g., customer or supplier) who participates.



AGENTS

- What agents are involved in the sale?

Take Order

Inventory

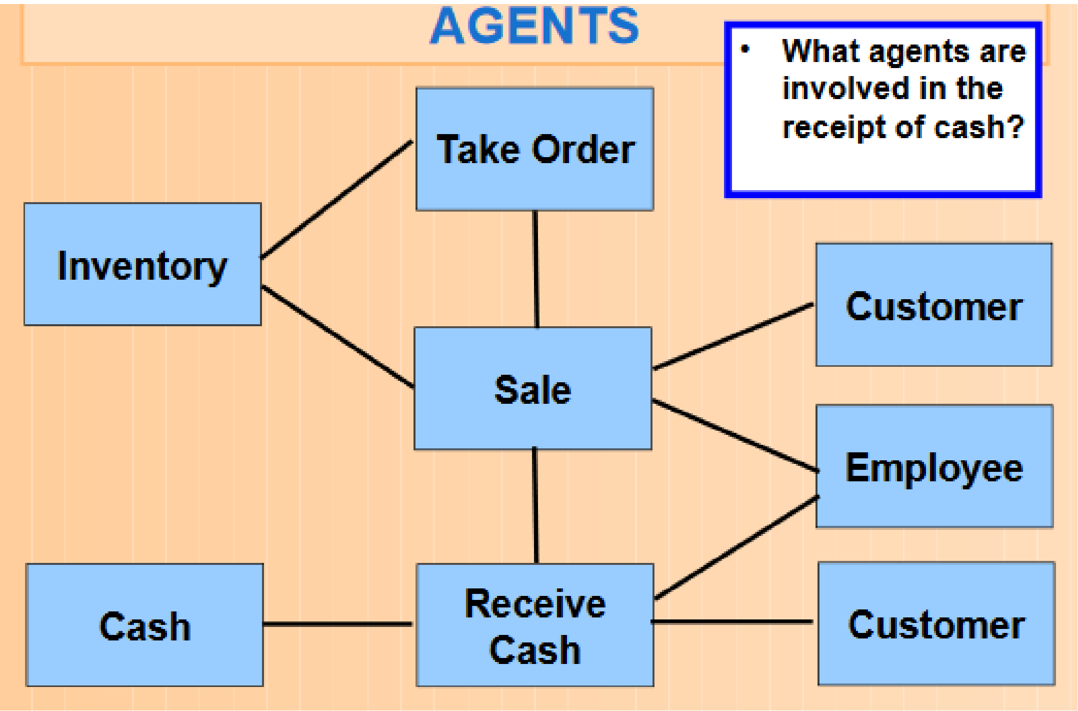
Customer

Sale

Employee

Cash

Receive Cash



AGENTS

- What agents are involved in the receipt of cash?

Take Order

Inventory

Customer

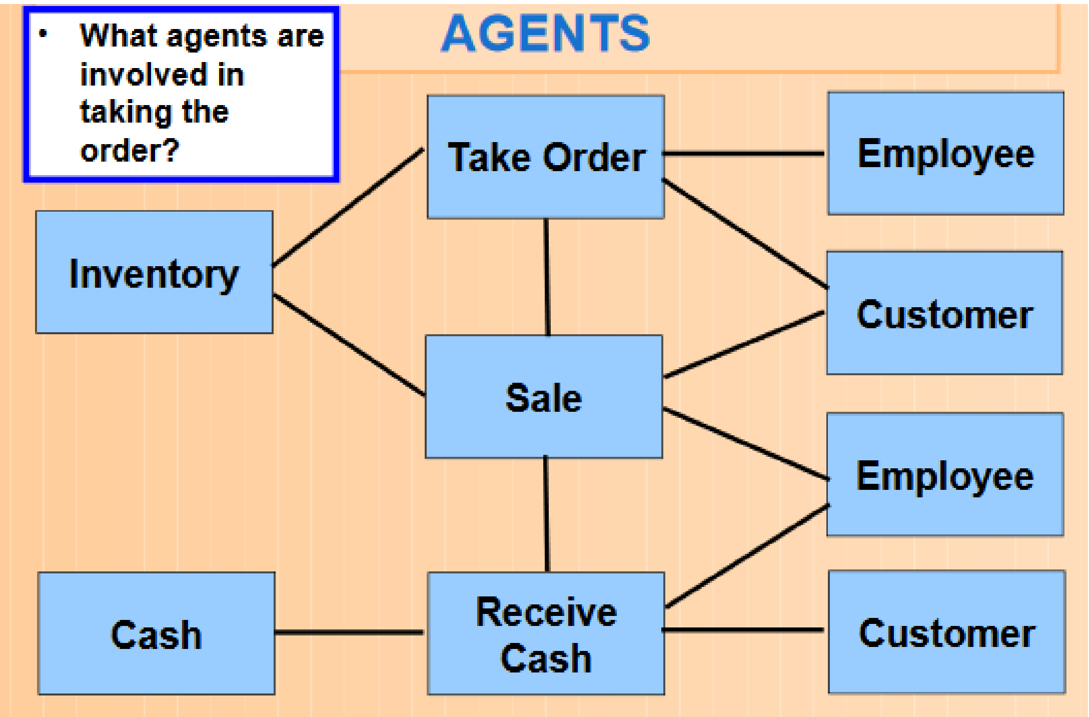
Sale

Employee

Cash

Receive Cash

Customer



- What agents are involved in taking the order?

AGENTS

STEP THREE: Determine the cardinalities between the relationships.

STEP THREE: DETERMINE CARDINALITIES OF RELATIONSHIPS

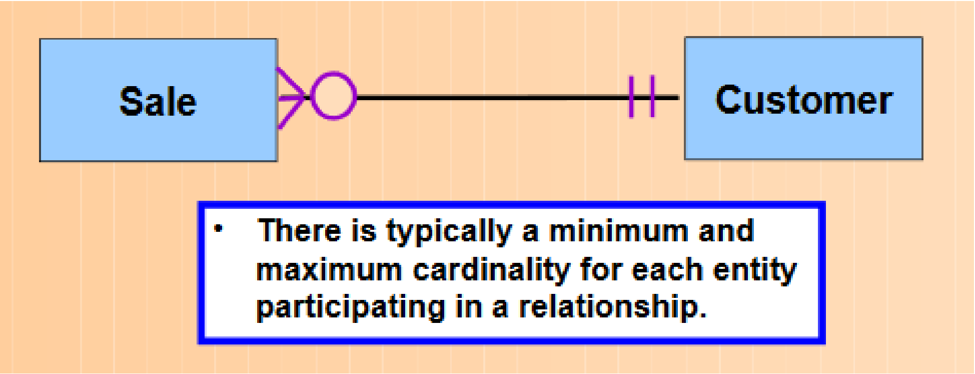
The final step in an REA diagram for a transaction cycle is to add information about the relationship cardinalities.

A *cardinality* describes the nature of the relationship between two entities.

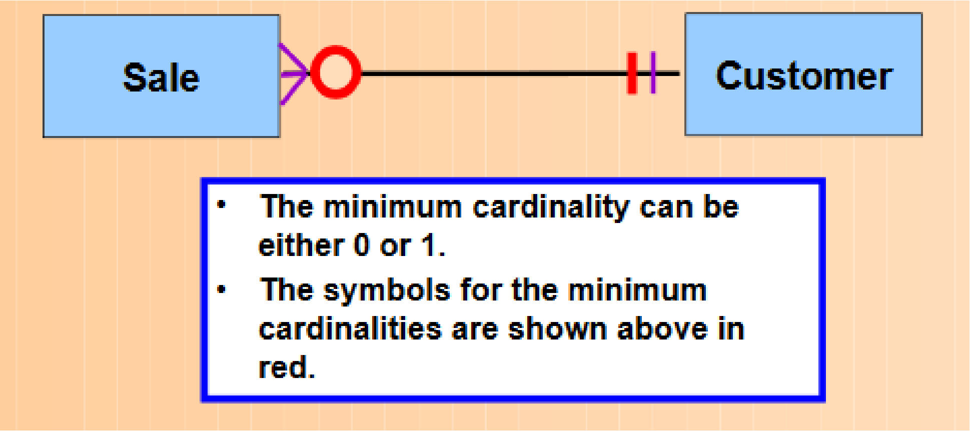
- It indicates how many instances of one entity can be linked to a specific instance of another entity.
- For example, the cardinality between the event ***Sales*** and the agent ***Customer*** answers the question:
  • For each sale a company makes, how many customers are associated with that sale?
- Unfortunately, there is no universal standard for diagramming cardinalities.
- In this text, we adopt the graphical “crow’s feet” notation style because:
  - It is becoming increasingly popular.
  - It is used by many software design tools.

Using the crow’s feet notation:

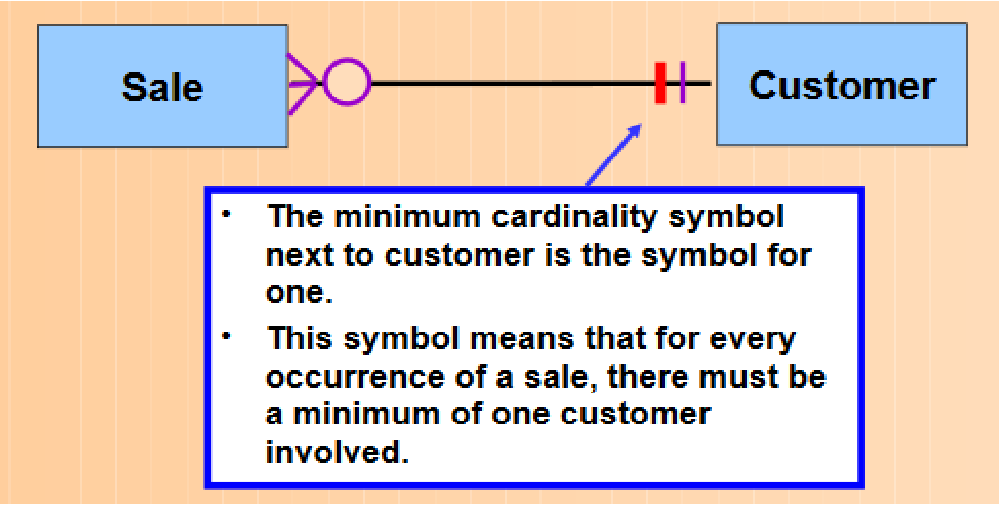
- The symbol for **zero** is a circle: **O**
- The symbol for **one** is a single stroke: **|**
- The symbol for many is the crow’s foot: <



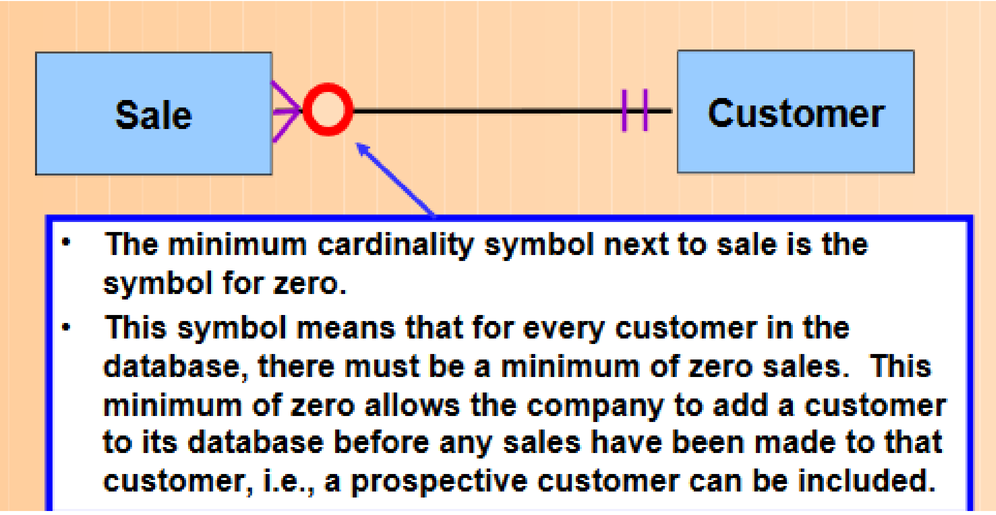
- There is typically a minimum and maximum cardinality for each entity participating in a relationship.



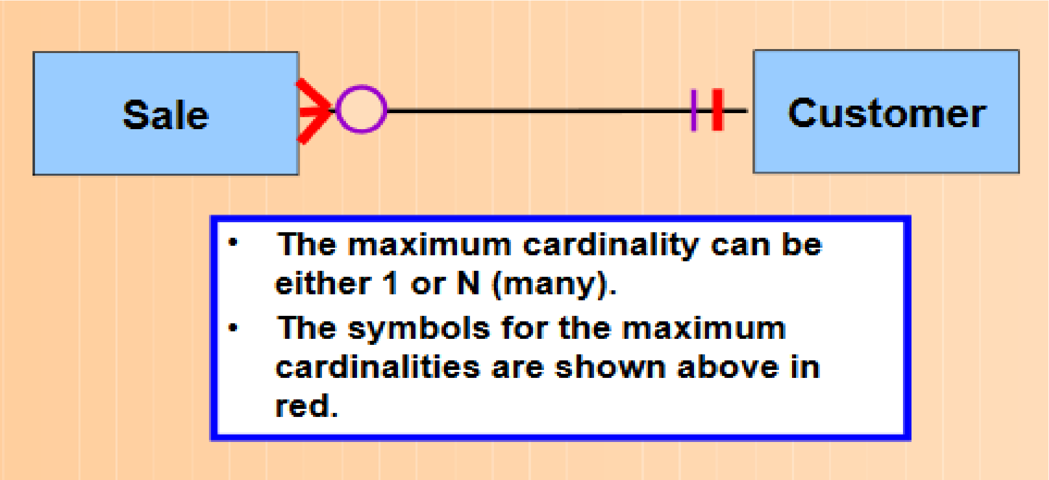
- The minimum cardinality can be either 0 or 1.
- The symbols for the minimum cardinalities are shown above in red.



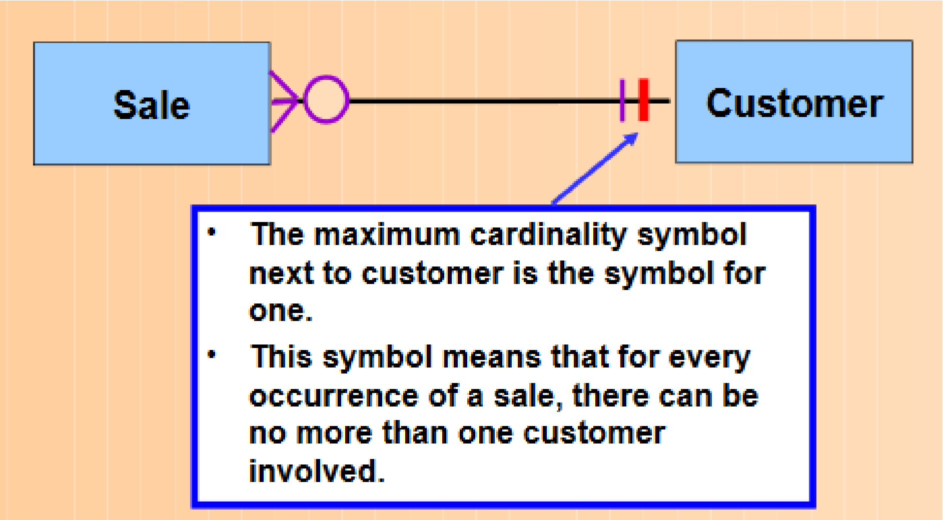
- The minimum cardinality symbol next to customer is the symbol for one.
- This symbol means that for every occurrence of a sale, there must be a minimum of one customer involved.



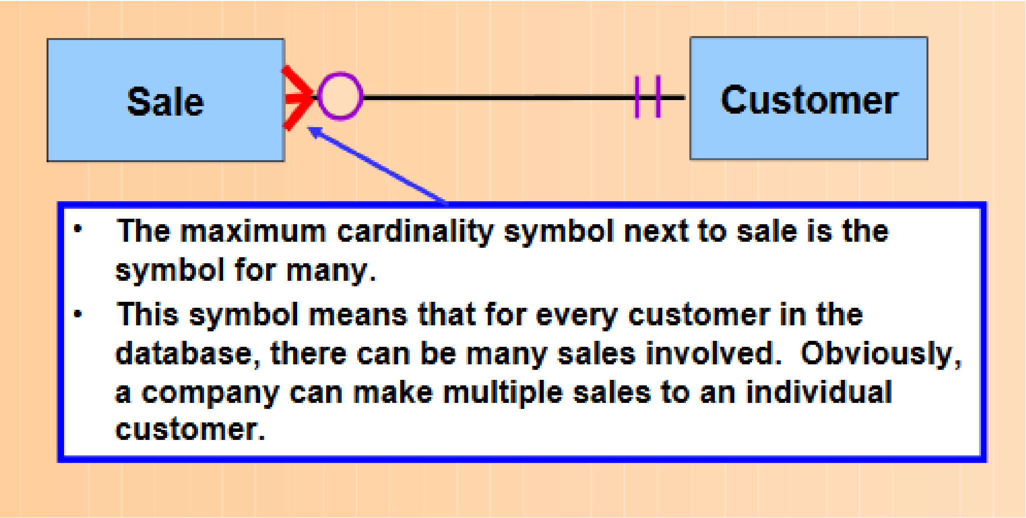
- The minimum cardinality symbol next to sale is the symbol for zero.
- This symbol means that for every customer in the database, there must be a minimum of zero sales. This minimum of zero allows the company to add a customer to its database before any sales have been made to that customer, i.e., a prospective customer can be included.



- The maximum cardinality can be either 1 or N (many).
- The symbols for the maximum cardinalities are shown above in red.



- The maximum cardinality symbol next to customer is the symbol for one.
- This symbol means that for every occurrence of a sale, there can be no more than one customer involved.

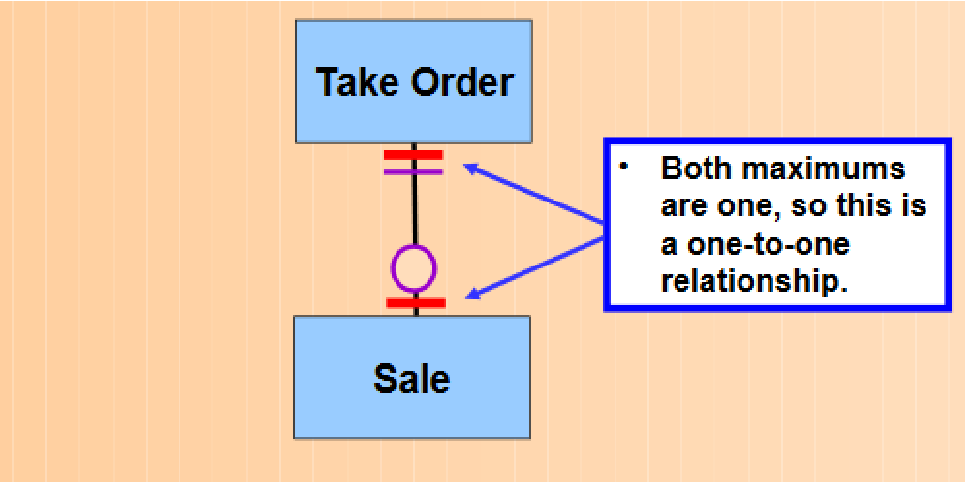


- The maximum cardinality symbol next to sale is the symbol for many.
- This symbol means that for every customer in the database, there can be many sales involved. Obviously, a company can make multiple sales to an individual customer.

Three Types of Relationships

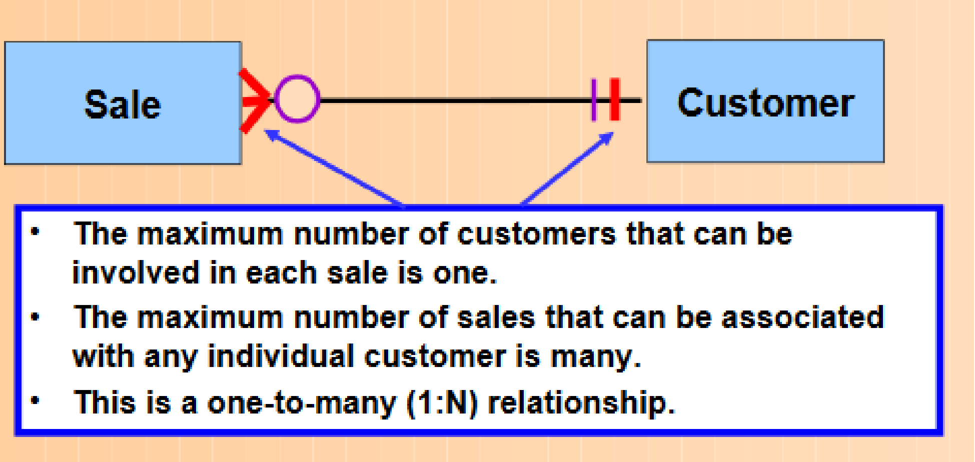
Three types of relationships are possible between entities.–Relationships depend on the maximum cardinality on each side of a relationship.

- **A one-to-one relationship (1:1) exists when the maximum cardinality for each entity in the relationship is 1.**



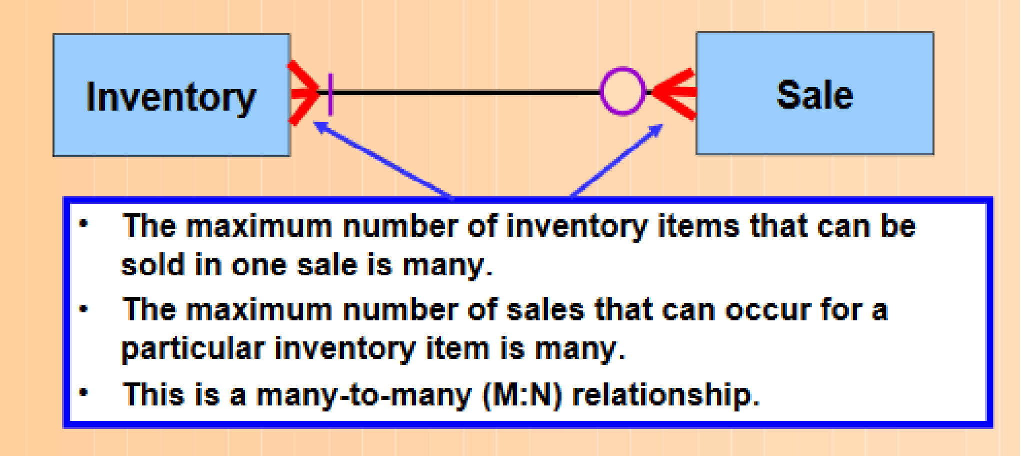
- Both maximums are one, so this is a one-to-one relationship.

A one-to-many (1:N) relationship exists when the maximum cardinality on one side is 1 and the maximum on the other side is many.



- The maximum number of customers that can be involved in each sale is one.
- The maximum number of sales that can be associated with any individual customer is many.
- This is a one-to-many (1:N) relationship.

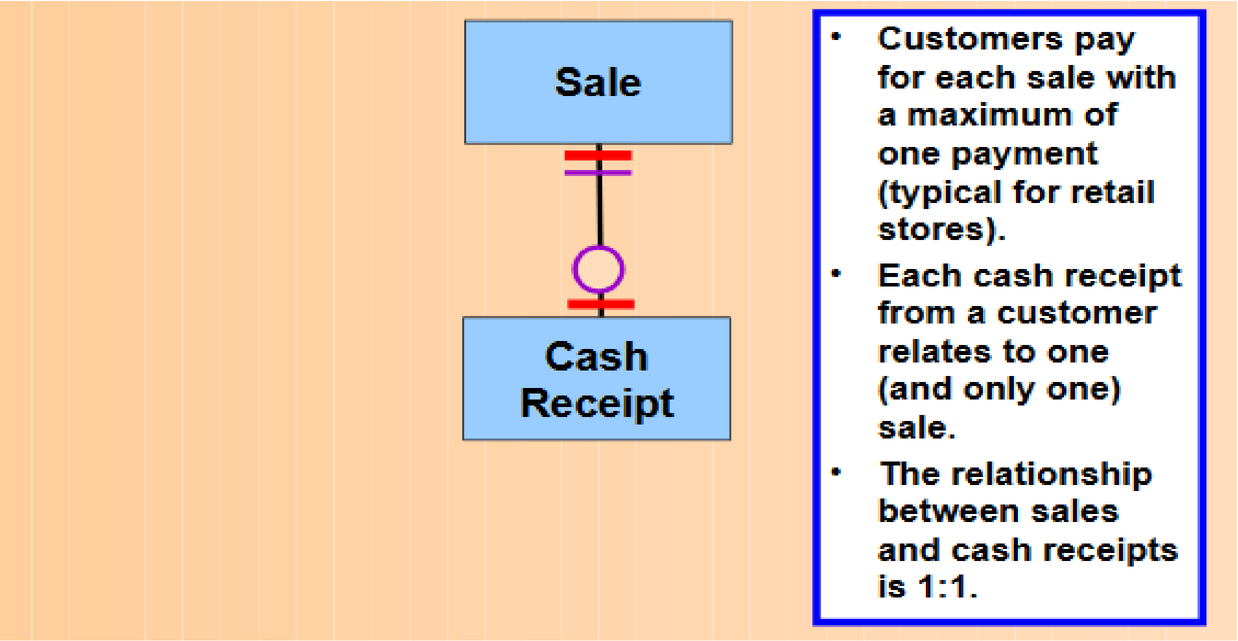
A many-to-many (M:N) relationship exists when the maximum on both sides is many.



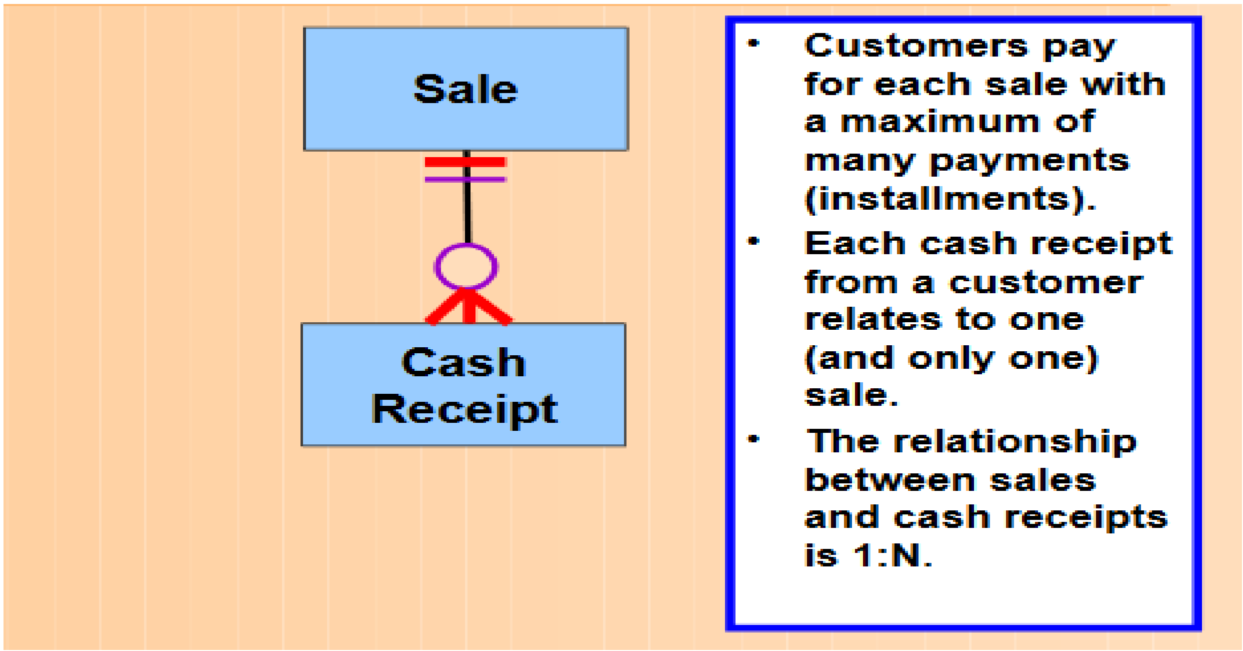
- The maximum number of inventory items that can be sold in one sale is many.
- The maximum number of sales that can occur for a particular inventory item is many.
- This is a many-to-many (M:N) relationship.

It is not a “one size fits all” world for relationships and cardinalities. The cardinalities between two entities can vary based on how the particular company does business.

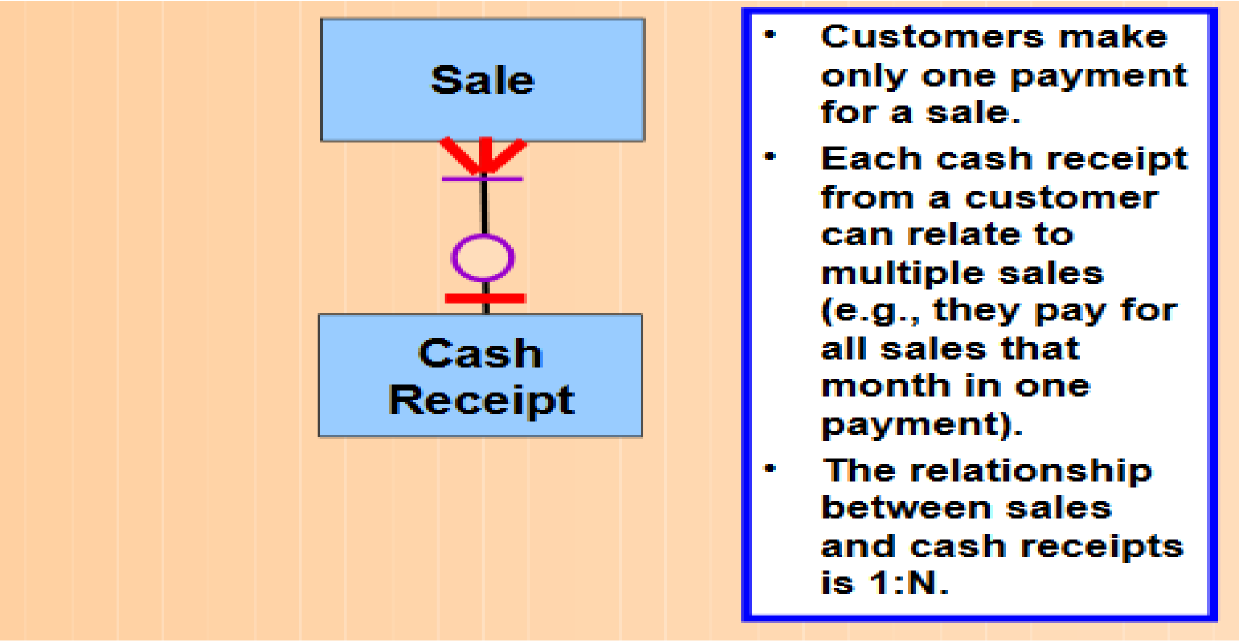
Let’s look at some examples.



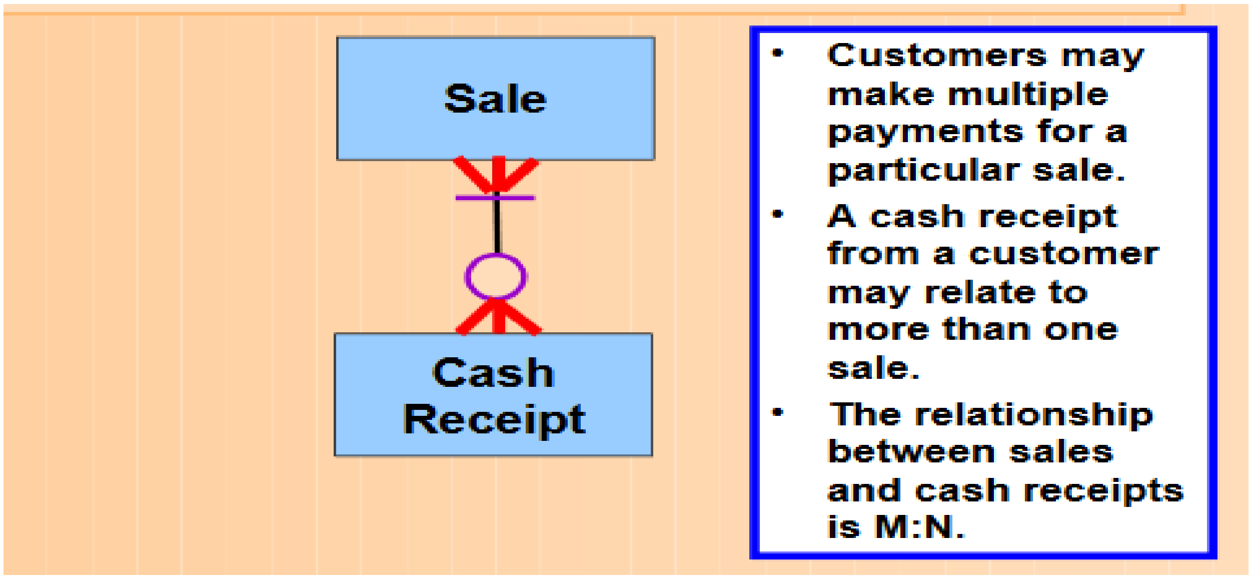
- Customers pay for each sale with a maximum of one payment (typical for retail stores).
- Each cash receipt from a customer relates to one (and only one) sale.
- The relationship between sales and cash receipts is 1:1.



- Customers pay for each sale with a maximum of many payments (installments).
- Each cash receipt from a customer relates to one (and only one) sale.
- The relationship between sales and cash receipts is 1:N.



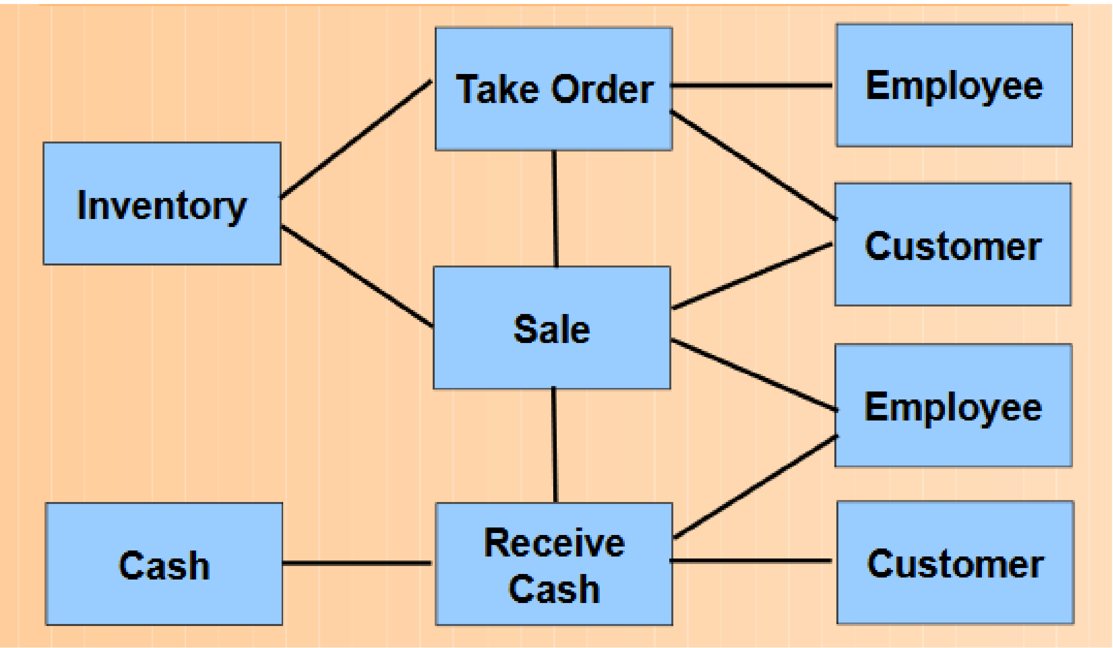
- Customers make only one payment for a sale.
- Each cash receipt from a customer can relate to multiple sales (e.g., they pay for all sales that month in one payment).
- The relationship between sales and cash receipts is 1:N.



- Customers may make multiple payments for a particular sale.
- A cash receipt from a customer may relate to more than one sale.
- The relationship between sales and cash receipts is M:N.

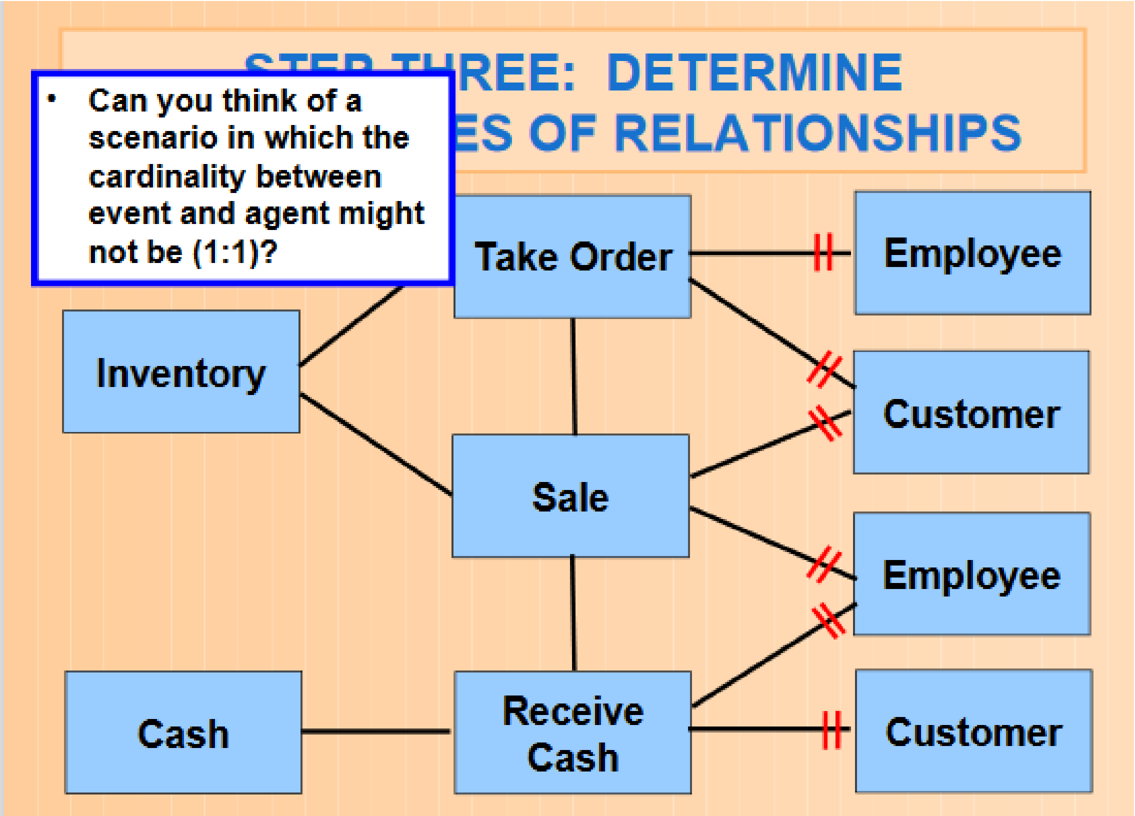
In other words, the choice of cardinalities is not arbitrary. It reflects facts about the organization that are obtained during the requirements definition stage of the database design process. Now let's go back to the REA diagram for the revenue cycle and see if we can complete the cardinalities.

Now let's go back to the REA diagram for the revenue cycle and see if we can complete the cardinalities



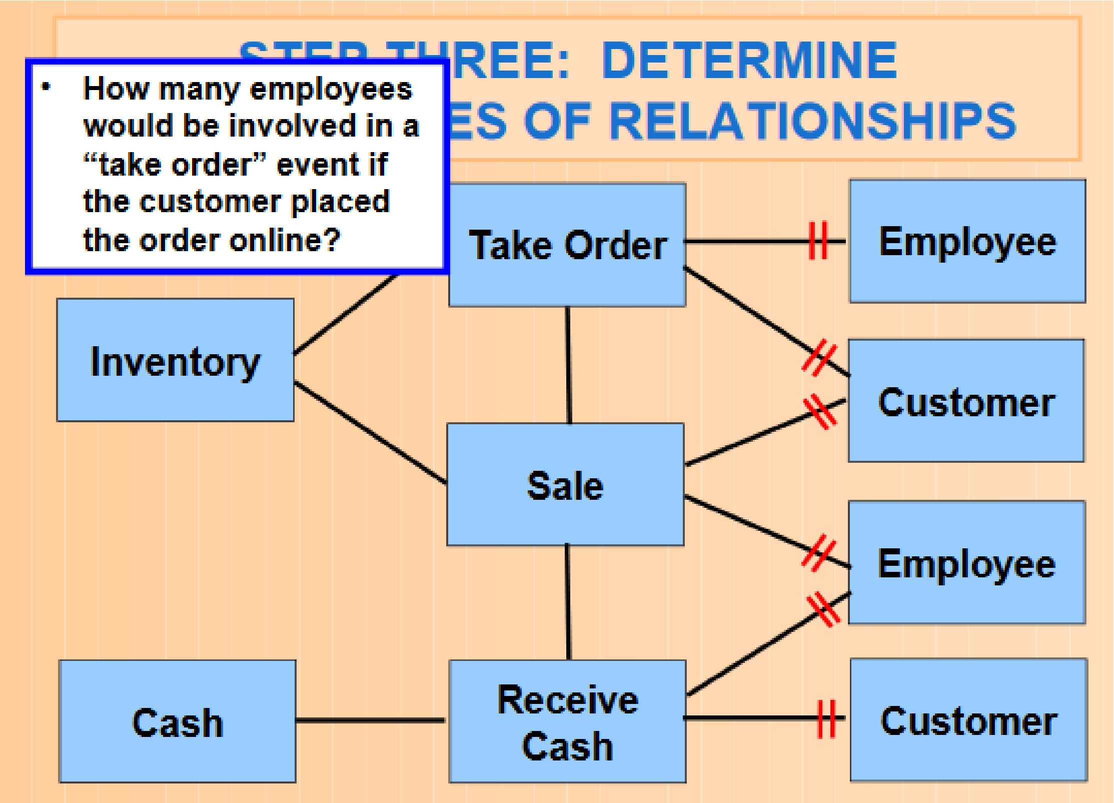
In relationships between events and agents:

- For each event that occurs, the cardinality between event and agent is typically (1:1).
- Example: When a sale occurs:
- There is usually one and only one customer.
- There is usually one and only one salesperson. This practice makes it more feasible for the organization to establish employee accountability for the event



STEP THREE: DETERMINE
ES OF RELATIONSHIPS

- Can you think of a scenario in which the cardinality between event and agent might not be (1:1)?

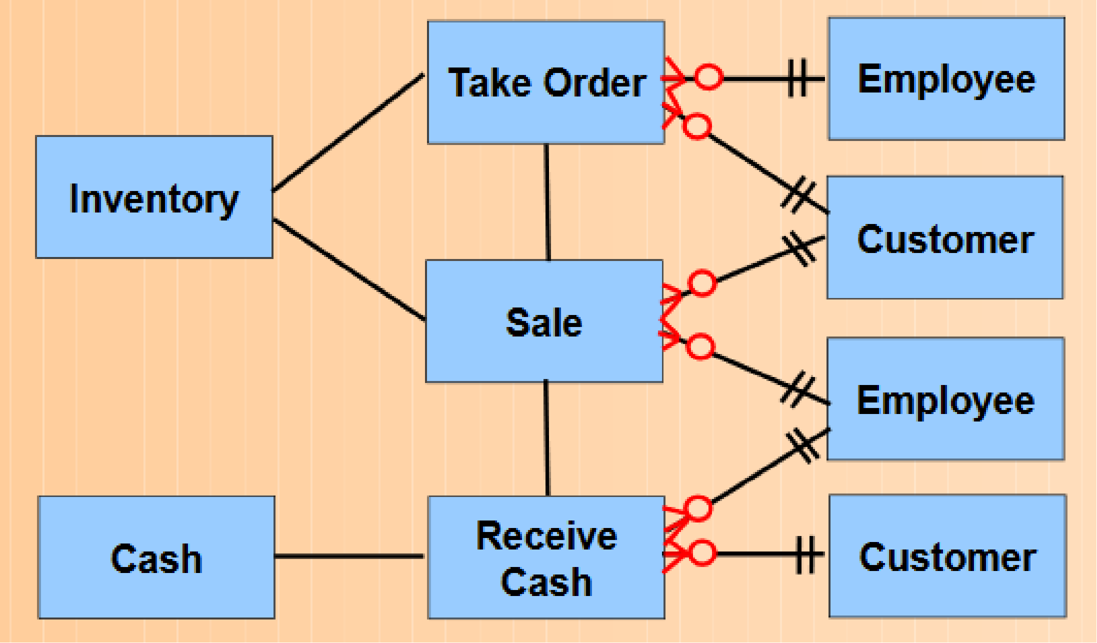


STEP THREE: DETERMINE
ES OF RELATIONSHIPS

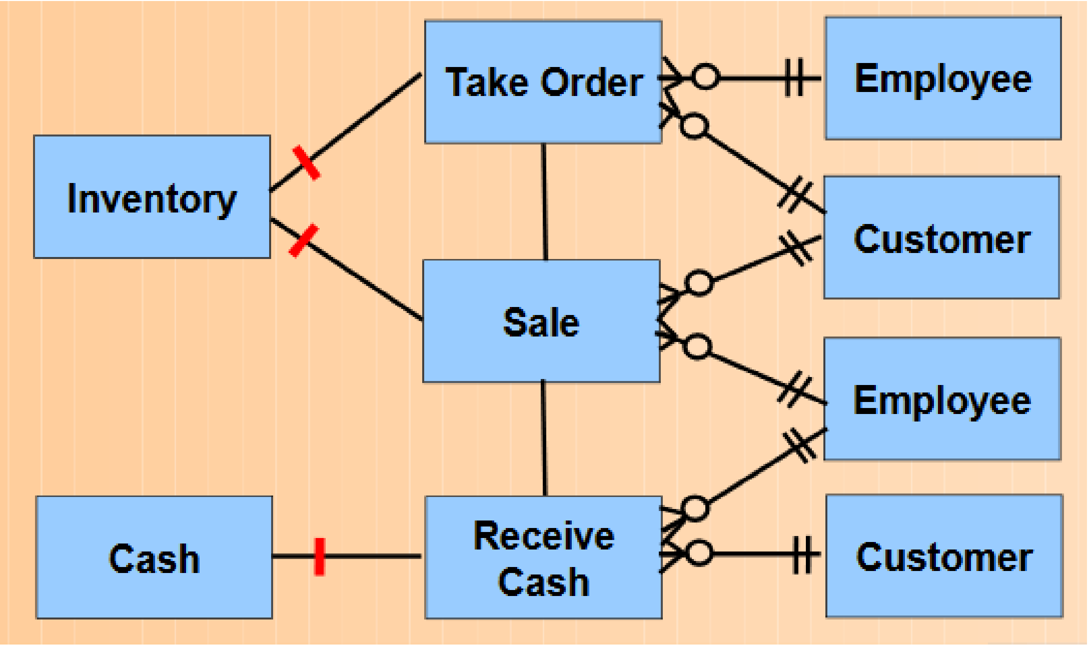
- How many employees would be involved in a “take order” event if the customer placed the order online?

For each agent the cardinality between agent and event is typically (0:N).

- Example: For a particular salesperson:
  •There is typically a minimum of zero sales (allows for inclusion of a new salesperson who has not yet made any sales). A salesperson can have a maximum of many sales.
- Or: For a particular customer:
  - There is typically a minimum of zero sales (to allow for the inclusion of prospective customers who haven't bought anything yet) and a maximum of many sales

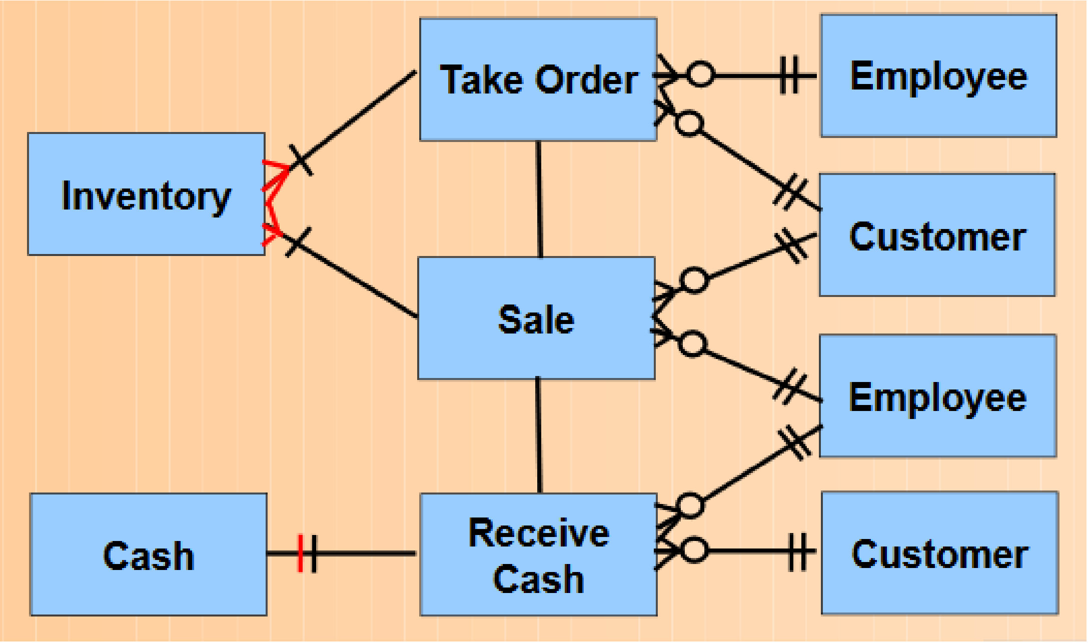


Let's now look at the relationship between events and resources. In the cardinality between event and resource, the minimum cardinality is typically one, because an event can't occur without affecting at least one resource.

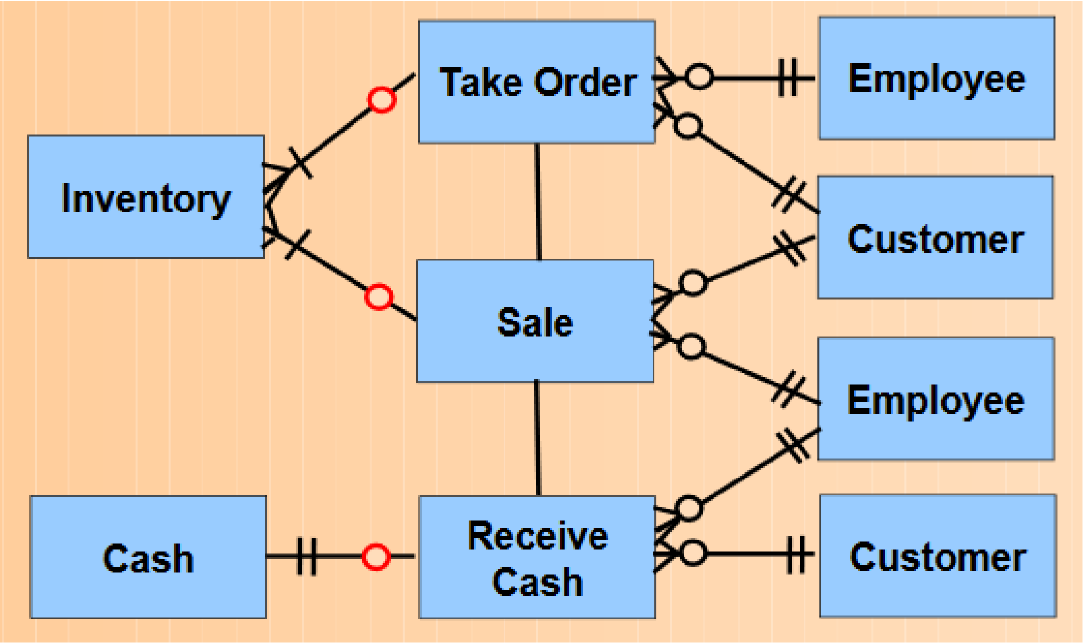


The maximum could be one or zero.

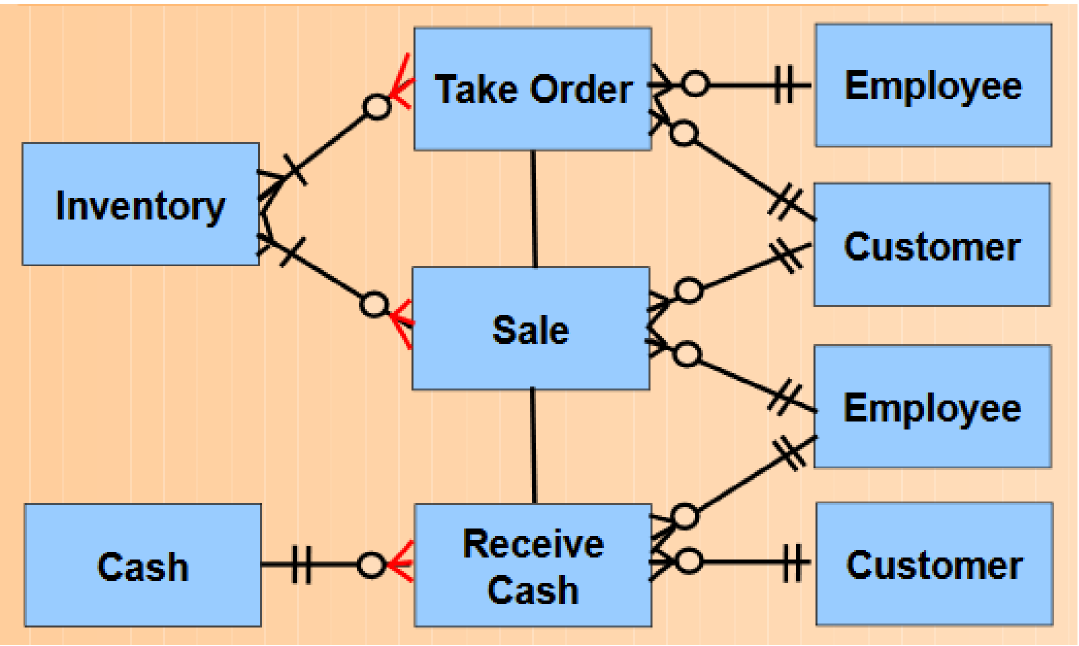
- In this particular story, each sale can involve many items of inventory, so the maximum is many. However, every receipt of cash is deposited to one and only one cash account, so the maximum there is one.



In the cardinality between event and resource, the minimum is typically zero.–A company can have an inventory item for which there has never been a sale.–When the company's cash account is new, there has never been a cash receipt deposited in it.



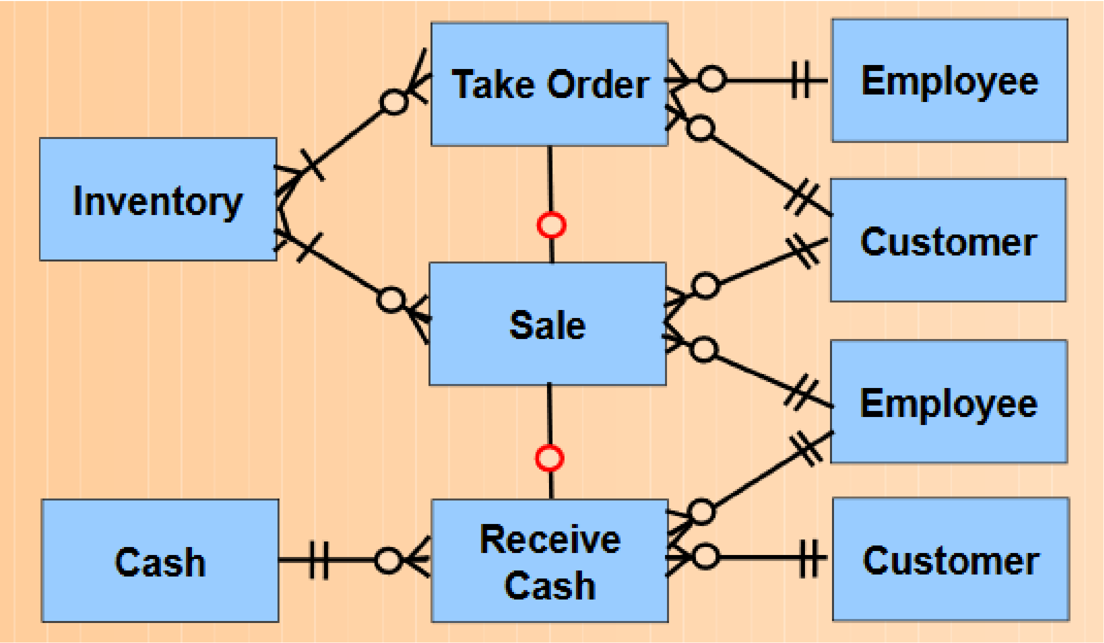
In the cardinality between event and resource, the maximum is typically many. Most inventory items can be sold many times. (An exception might occur if each inventory item is one unique item, such as a piece of real estate.) The company's cash account can have many cash receipts.



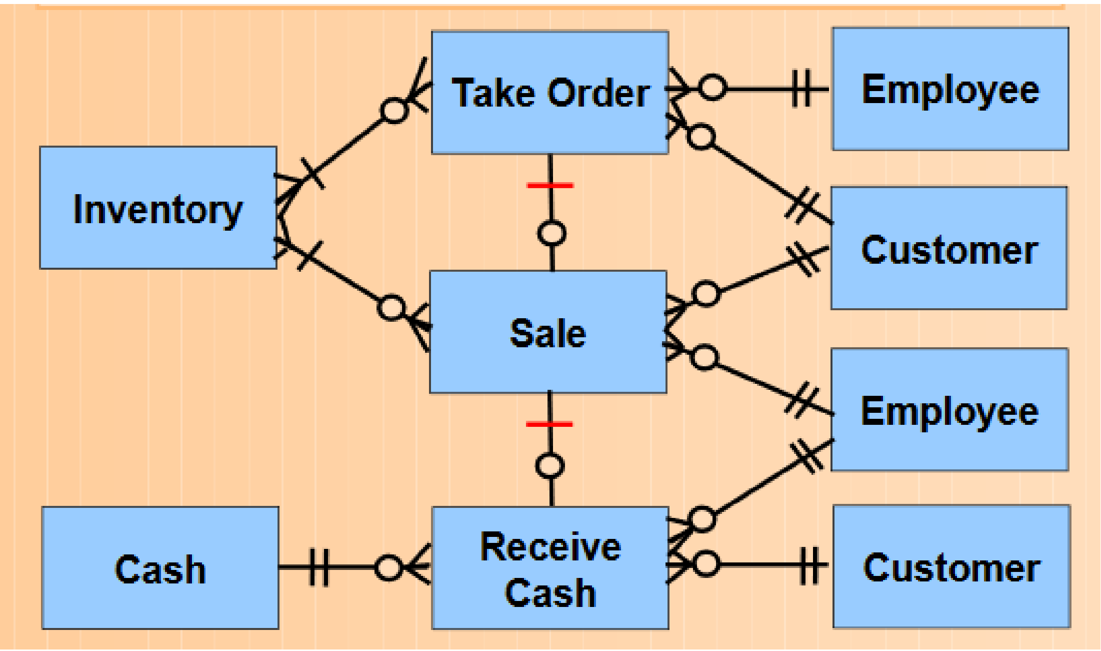
Finally, let's look at the relationships between events. When events occur in a sequence, the minimum cardinality between the first event and the second event is always zero, because there is a span of time (although possibly quite short) when the first event has occurred but there are zero occurrences of the second event.

Examples:

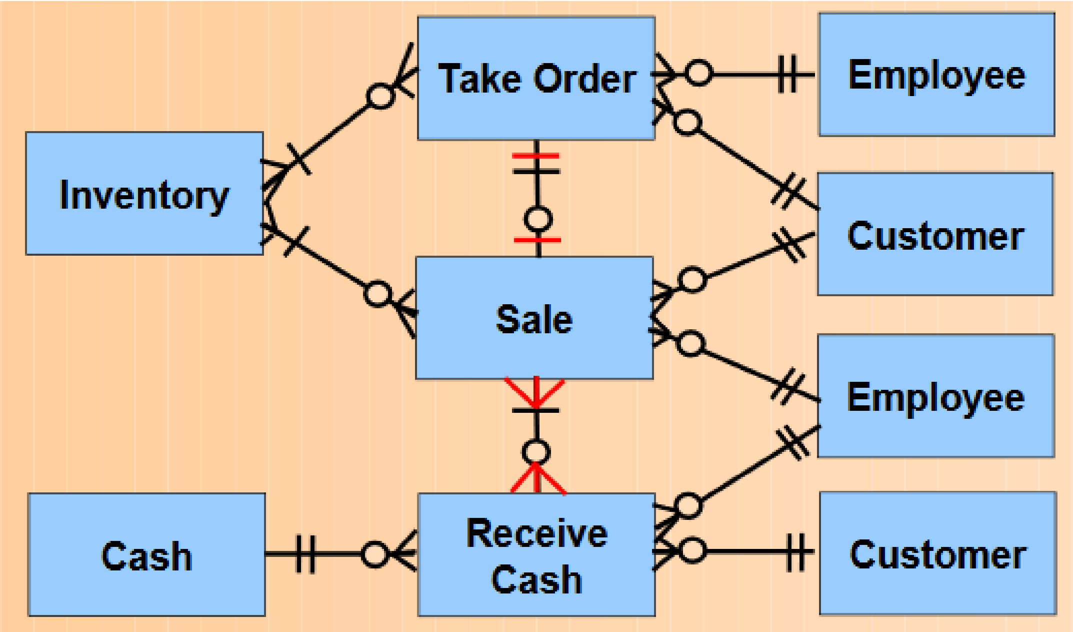
When an order is first taken, there have been no deliveries of goods (sale event) to the customer. When goods are delivered to the customer, there is a span of time, however brief, in which there is no cash receipt from the customer.



The minimum cardinality between the second event and the first event is typically one, because the second event can't occur without the first event having occurred.



An exception could occur if the first event is not required for the second event to occur. Example: If a sale can be made without first taking an order, then the minimum cardinality between ***Sale*** and ***take order*** could be zero. The maximums in the cardinalities between events can be either one or many, and these maximums vary based on business practices. We saw this when we looked at the four different possibilities for the relationships between sales and cash receipts previously. On the following slides, see if you can explain the maximums between the three events.



Uniqueness of REA Diagrams

Each organization will have its own unique REA diagram. Business practices differ across companies, so cardinalities and relationships will differ. A given organization can change business practices, leading to a change in its REA diagram: A change in practice could cause a change in cardinalities. Could even lead to the inclusion of different entities on the diagram.

Data modeling can be complex and repetitive.

Data modelers must discuss their drafts of models with intended users to ensure that: Key dimensions are not omitted or misunderstood. Terminology is consistent.

4.4 Summary

In this chapter, you've learned about the steps to follow in designing and implementing a database system.

You've learned how the REA data model is used to design an AIS database and how an entity-relationship diagram of an AIS database is drawn.

You've also learned how to read REA diagrams and what they reveal about the activities and policies of the organization being modeled.

Unit Questions

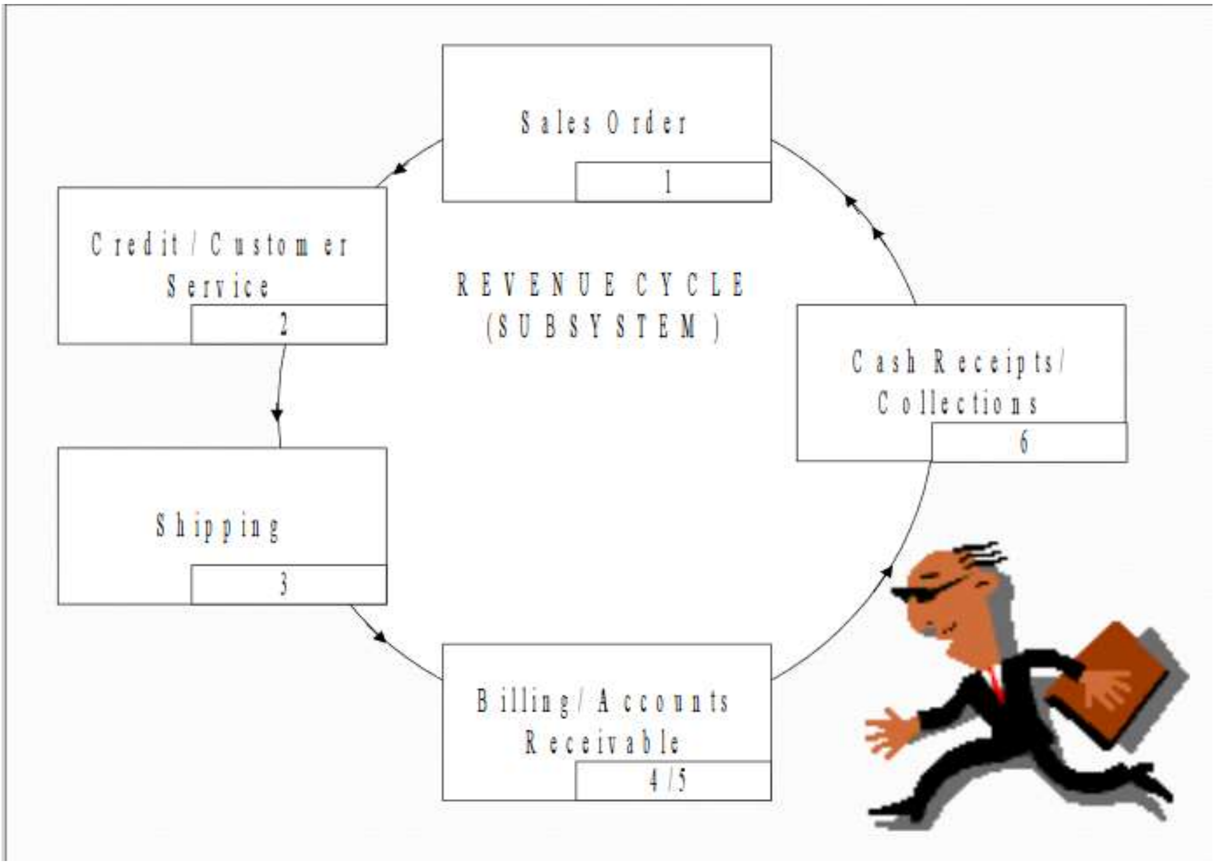
1. What are the database design steps?
2. Discuss how accountants can participate in the design of an AIS.

3. Name three types of REA MODEL entity categories.
4. What are the two important tools that facilitate data modeling.
5. Name the basic REA template in structuring relationships.
6. Discuss the principle of cardinalities by using one to many, many to many in detail.

4.5 REVENUE CYCLE

4.5.1 Objectives of revenue cycle

i. Tasks performed in the revenue cycle, regardless of the technology used
ii. Functional departments in the revenue cycle and the flow of revenue transactions through the organization
iii. Documents, journals, and accounts needed for audit trails, records, decision making, and financial reporting
iv. Risks associated with the revenue cycle and the controls that reduce these risks
v. The operational and control implications of technology used to automate and reengineer the revenue cycle.


Sales Order
1
Credit / Customer Service
2
REVENUE CYCLE
(SUBSYSTEM)
Shipping
3
Billing / Accounts Receivable
4 / 5
Cash Receipts / Collections
6

Journal Vouchers/Entries. How do we get them?

Billing Department prepares a journal voucher:

Accounts Receivable	DR	
Sales		CR
Inventory Control Dept. prepares a journal voucher:		
Cost of Goods Sold	DR	
Inventory		CR
Cash Receipts prepares a journal voucher:		
Cash	DR	
Accounts Receivable		CR

4.5.2 Revenue Cycle Databases

a) Master files

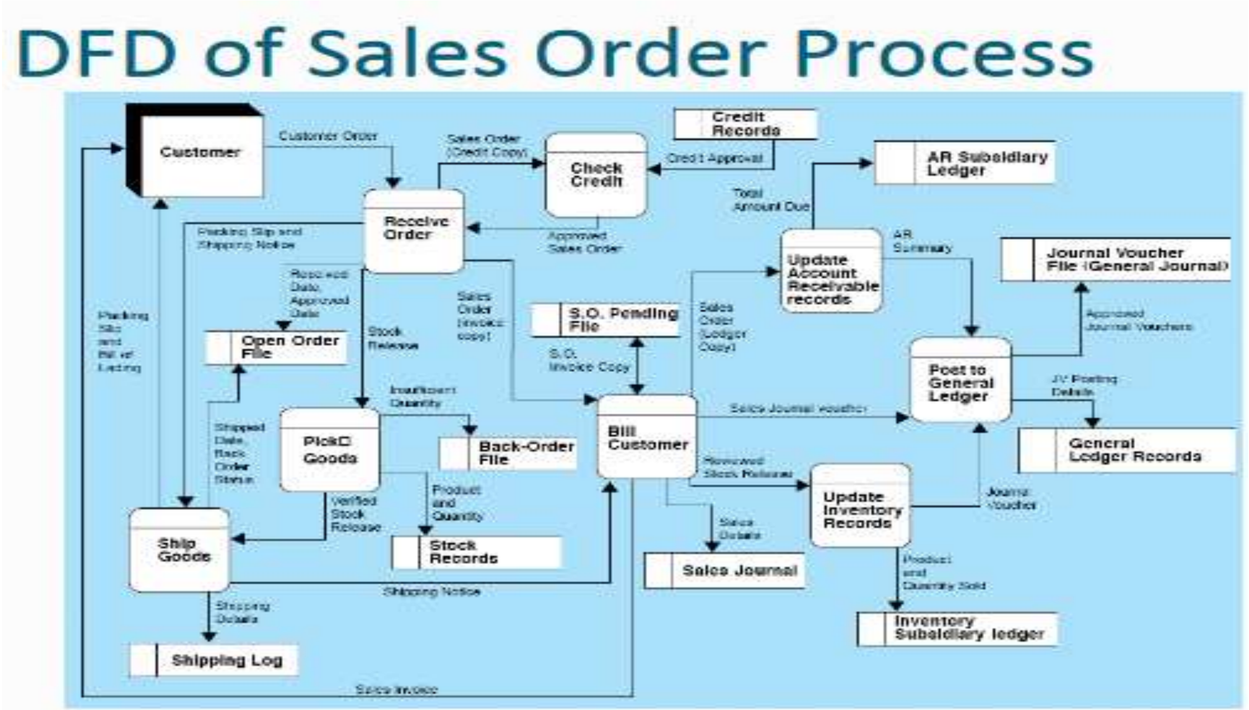
- Customer master file
- Accounts receivable master file
- Merchandise inventory master file

b) Transaction and Open Document Files

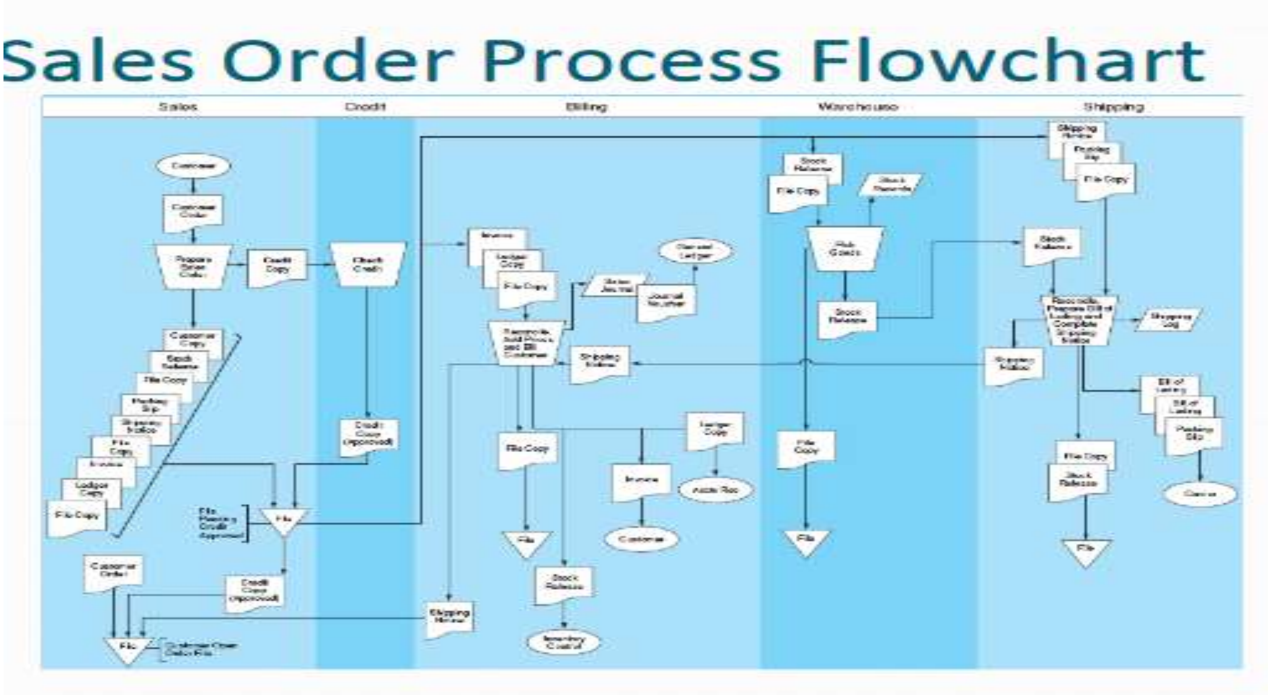
- Sales order transaction file
- Open sales order transaction file
- Sales invoice transaction file
- Cash receipts transaction file

c) Other Files

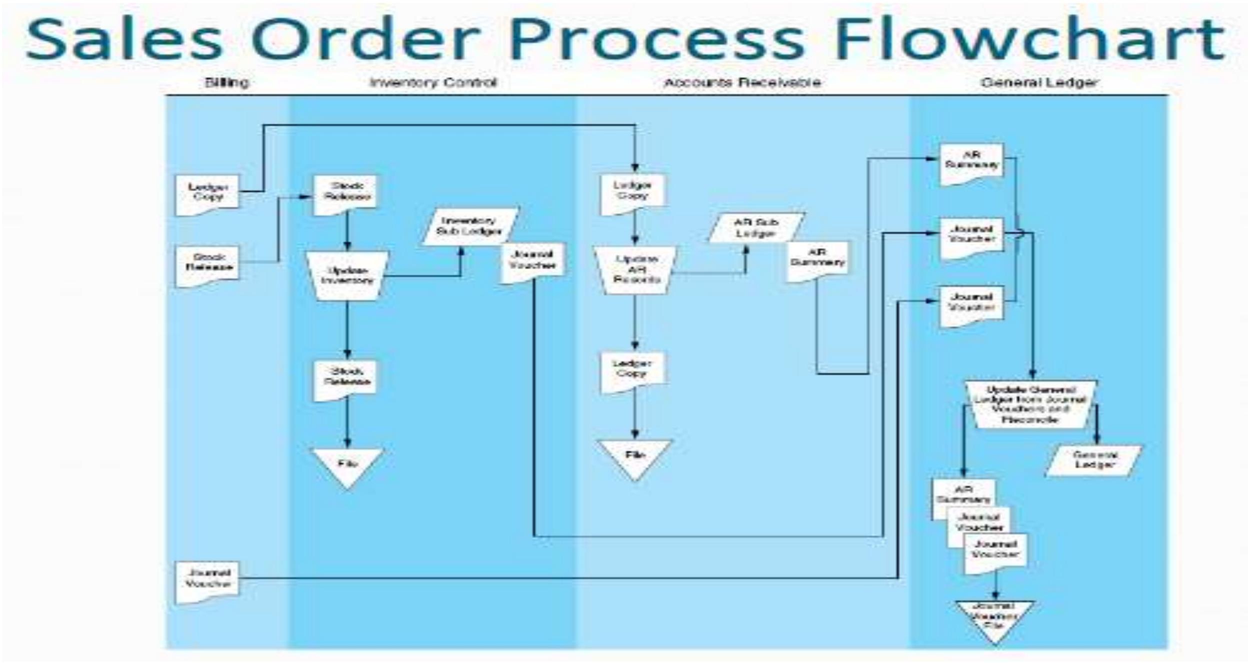
- Shipping and price data reference file
- Credit reference file (may not be needed)
- Salesperson file (may be a master file)
- Sales history file
- Cash receipts history file
- Accounts receivable reports file



Sales order process flowchart



Sales order process flowchart

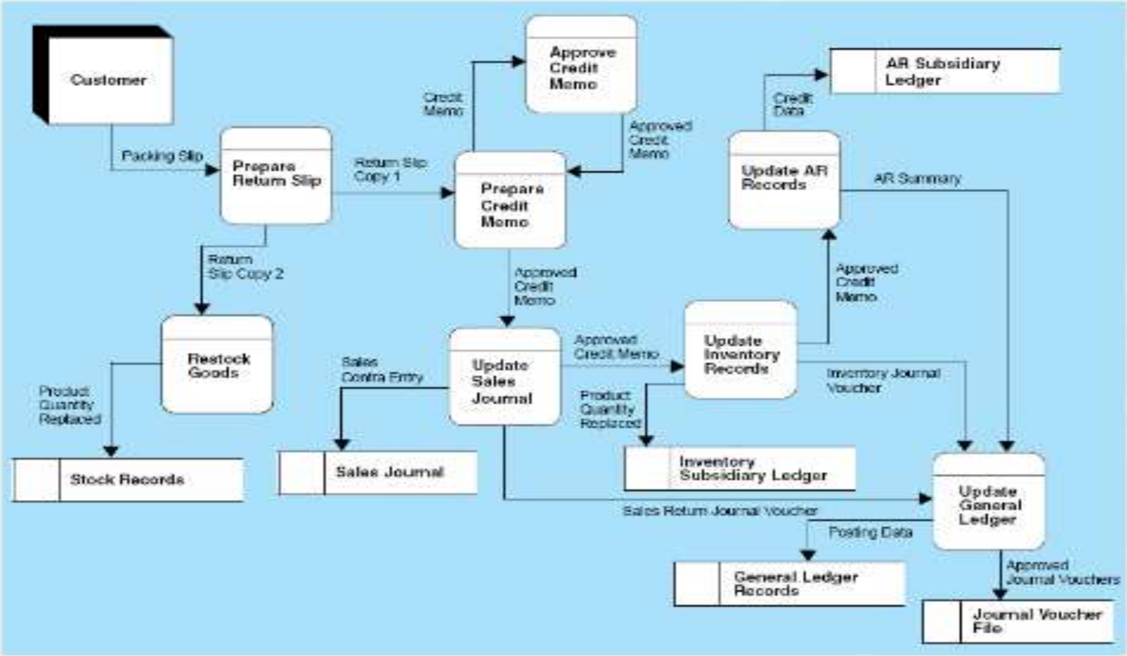


4.5.3 Manual Sales Order Processing

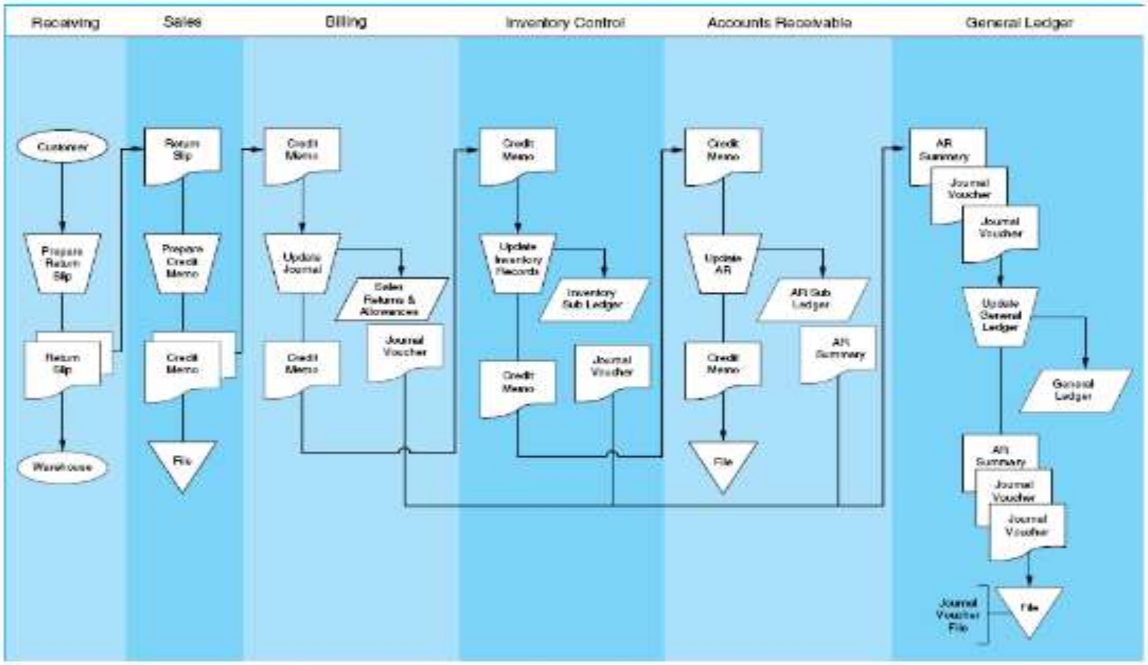
- Begins with a customer placing an order
  - The sales department captures the essential details on a sales order form.
- The transaction is authorized by obtaining credit approval by the credit department.
- Sales information is released to:
  - Billing
  - Warehouse (stock release or picking ticket)
  - Shipping (packing slip and shipping notice)
- The merchandise is picked from the Warehouse and sent to Shipping.
  - Stock records are adjusted.
- The merchandise, packing slip, and bill of lading are prepared by Shipping and sent to the customer.
  - Shipping reconciles the merchandise received from the Warehouse with the sales information on the packing slip.
- Shipping information is sent to Billing. Billing compiles and reconciles the relevant facts and issues an invoice to the customer and updates the sales journal. Information is transferred to:
  - Accounts Receivable (A/R)
  - Inventory Control
- A/R records the information in the customer's account in the accounts receivable subsidiary ledger.
- Inventory Control adjusts the inventory subsidiary ledger.

- Billing, A/R, and Inventory Control submits summary information to the General Ledger dept., which then reconciles this data and posts to the control accounts in the G/L.

DFD of Sales Returns



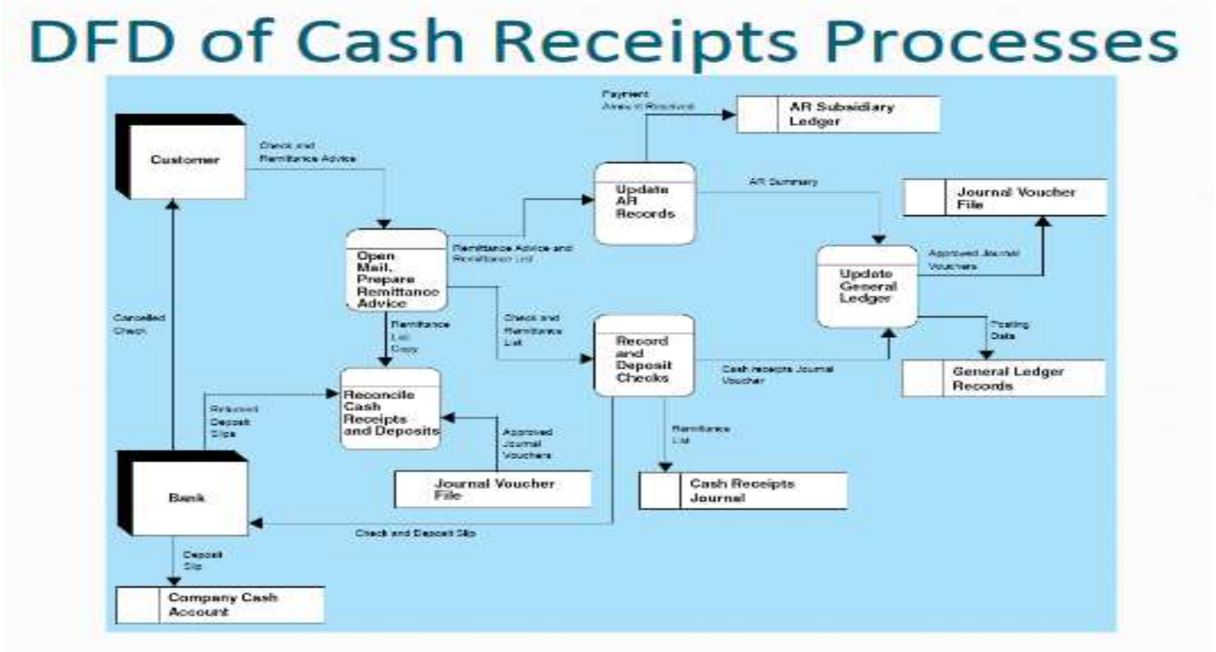
Sales Returns Flowchart



Sales Return Journal Entry

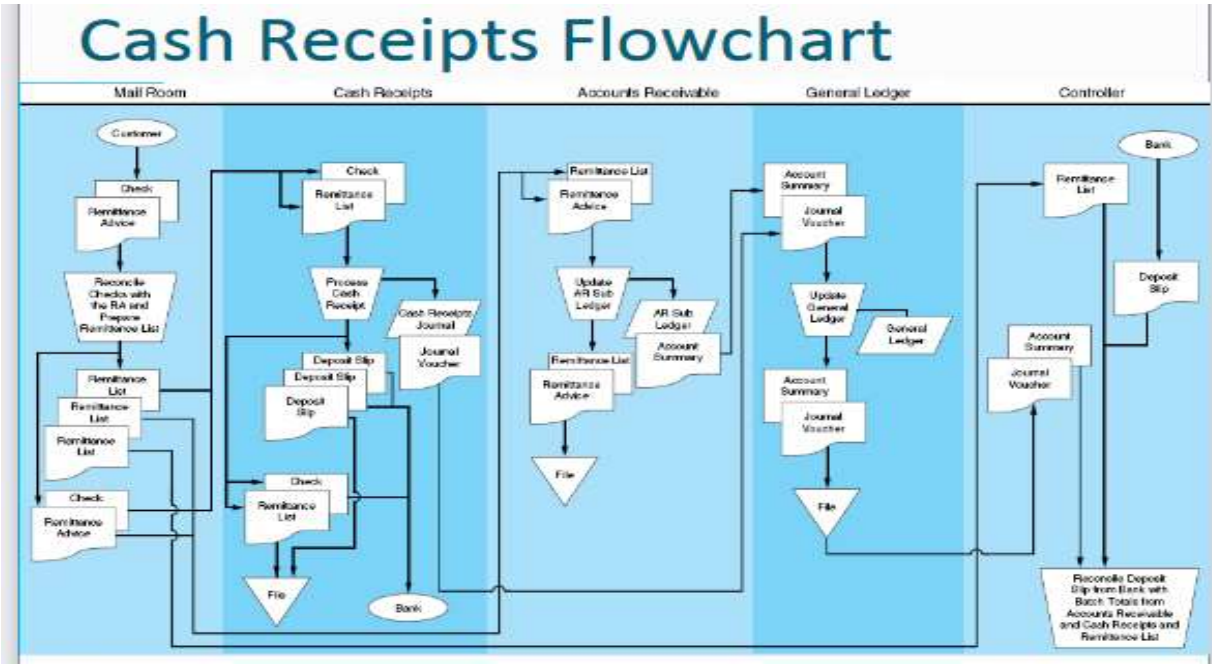
G/L posts the following to control accounts:

Inventory—Control Sales	Dr	
Sales Returns and Allowances	Dr	
Cost Of Goods Sold		Cr
Accounts Receivable—Control		Cr



DFD of Cash Receipts Processes

Cash Receipts Flowchart



Cash Receipts Flowchart

4.5.4 Manual Cash Receipts Processes

Customer checks and remittance advices are received in the Mail Room.

- A mail room clerk prepares a cash prelist and sends the prelist and the checks to Cash Receipts.
- The cash prelist is also sent to A/R and the Controller.

Cash Receipts:

- Verifies the accuracy and completeness of the checks
- Updates the cash receipts journal
- Prepares a deposit slip
- Prepares a journal voucher to send to G/L

A/R posts from the remittance advices to the accounts receivable subsidiary ledger.

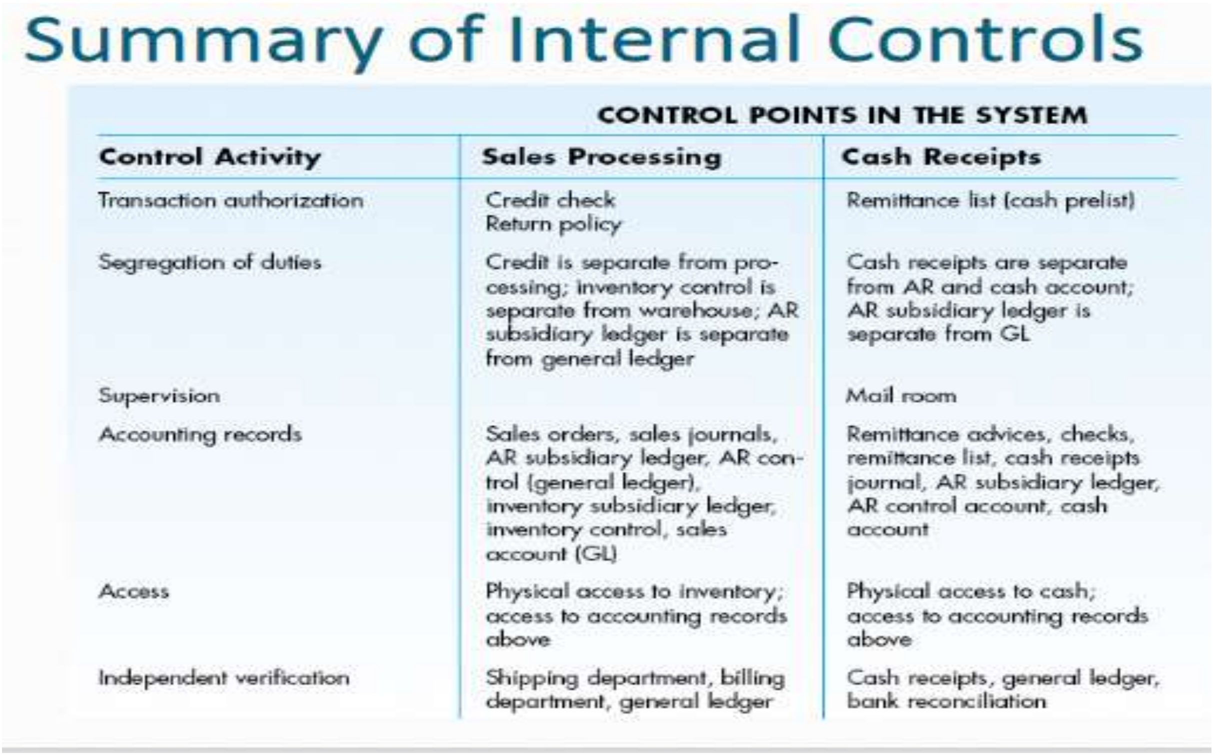
- Periodically, a summary of the postings is sent to G/L.

G/L department:

- Reconciles the journal voucher from Cash Receipts with the summaries from A/R
- Updates the general ledger control accounts

The Controller reconciles the bank accounts.

Summary of Internal Controls



Summary of Internal Controls

	CONTROL POINTS IN THE SYSTEM	
Control Activity	Sales Processing	Cash Receipts
Transaction authorization	Credit check Return policy	Remittance list (cash prelist)
Segregation of duties	Credit is separate from processing; inventory control is separate from warehouse; AR subsidiary ledger is separate from general ledger	Cash receipts are separate from AR and cash account; AR subsidiary ledger is separate from GL
Supervision		Mail room
Accounting records	Sales orders, sales journals, AR subsidiary ledger, AR control (general ledger), inventory subsidiary ledger, inventory control, sales account (GL)	Remittance advices, checks, remittance list, cash receipts journal, AR subsidiary ledger, AR control account, cash account
Access	Physical access to inventory; access to accounting records above	Physical access to cash; access to accounting records above
Independent verification	Shipping department, billing department, general ledger	Cash receipts, general ledger, bank reconciliation

4.5.5 Authorization Controls

Proper authorization of transactions (documentation) should occur so that only valid transactions get processed. Within the revenue cycle, authorization should take place when:

- a sale is made on credit (authorization)
- a cash refund is requested (authorization)
- posting a cash payment received to a customer's account (cash pre-list)

Segregation of Functions

Three Rules

1. Transaction authorization should be separate from transaction processing.
2. Asset custody should be separate from asset record-keeping.
3. The organization should be so structured that the perpetration of a fraud requires collusion between two or more individuals.

a. **Sales Order Processing**
   - credit authorization separate from SO processing
   - inventory control separate from warehouse
   - accounts receivable sub-ledger separate from general ledger control account

b. **Cash Receipts Processing**

  - cash receipts separate from accounting records
  - accounts receivable sub-ledger separate from general ledger

Supervision

Often used when unable to enact appropriate segregation of duties. Supervision of employees serves as a deterrent to dishonest acts and is particularly important in the mailroom.

Accounting Records

With a properly maintained audit trail, it is possible to track transactions through the systems and to find where and when errors were made:

- pre-numbered source documents
- special journals
- subsidiary ledgers
- general ledger
- file

Access Controls

Access to assets and information (accounting records) should be limited.

Within the revenue cycle, the assets to protect are cash and inventories and access to records such as the accounts receivable subsidiary ledger and cash journal should be restricted.

Independent Verification

Physical procedures as well as record-keeping should be independently reviewed at various points in the system to check for accuracy and completeness:

- shipping verifies the goods sent from the warehouse are correct in type and quantity
- warehouse reconciles the stock release document (picking slip) and packing slip
- billing reconciles the shipping notice with the sales invoice
- General ledger reconciles journal vouchers from billing, inventory control, cash receipts, and accounts receivable.

Automating the Revenue Cycle

Authorizations and data access can be performed through computer screens. There is a decrease in the amount of paper. The manual journals and ledgers are changed to disk or tape transaction and master files. Input is still typically from a hard copy document and goes through one or more computerized processes. Processes store data in electronic files (the tape or disk) or prepare data in the form of a hardcopy report.

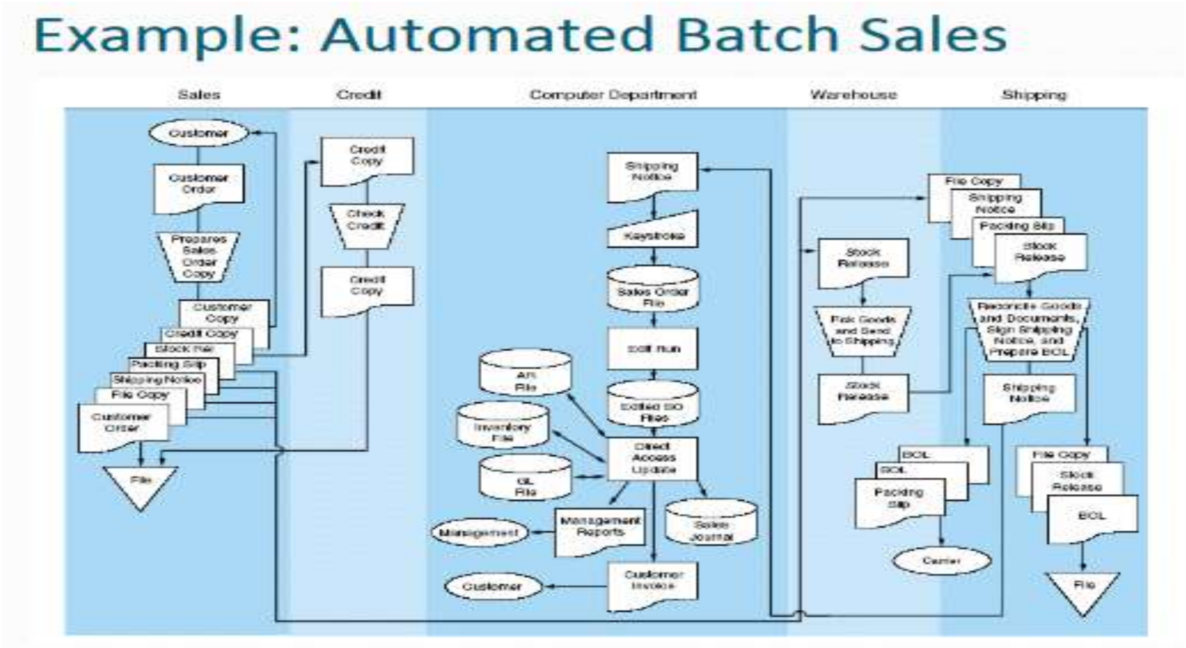
Revenue cycle programs can include: formatted screens for collecting data, edit checks on the data entered, instructions for processing and storing the data, security procedures (passwords or user IDs), steps for generating and displaying output.

To understand files, you must consider the record design and layout. The documents and the files used as input sources must contain the data necessary to generate the output reports.

4.6 Computer-Based Accounting Systems

CBAS technology can be viewed as a continuum with two extremes: ***Automation* -** use technology to improve efficiency and effectiveness; ***Reengineering*** – use technology to restructure business processes and firm organization.

Example: Automated Batch Sales



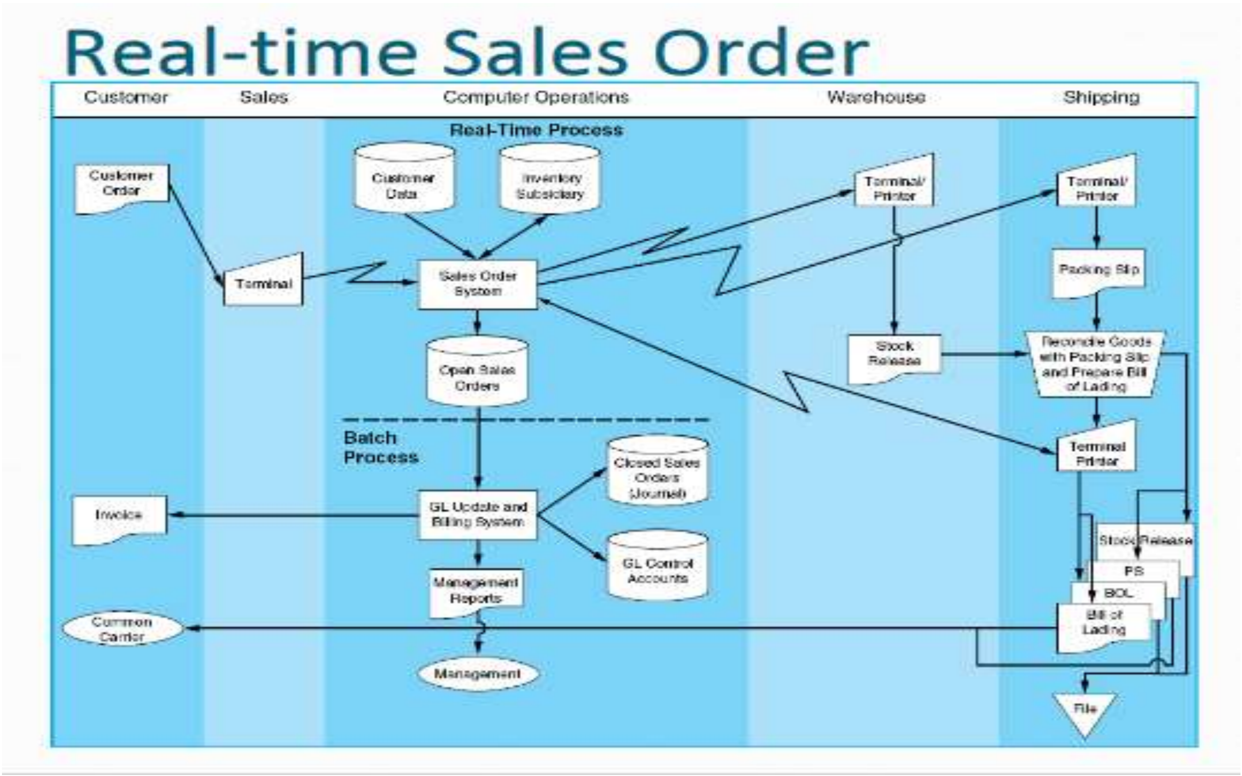
Reengineering Sales Order Processing Using Real-Time Technology

Manual procedures and physical documents are replaced by interactive computer terminals.

Real time input and output occurs, with some master files still being updated using batches.

- Real-time - entry of customer order, printout of stock release, packing slip and bill of lading; update of credit file, inventory file, and open sales orders file
- Batch - printout of invoice, update of closed sales order (journal), accounts receivable and general ledger control account

Real time sales order



Advantages of Real-Time Processing

i. Shortens the cash cycle of the firm by reducing the time between the order date and billing date.

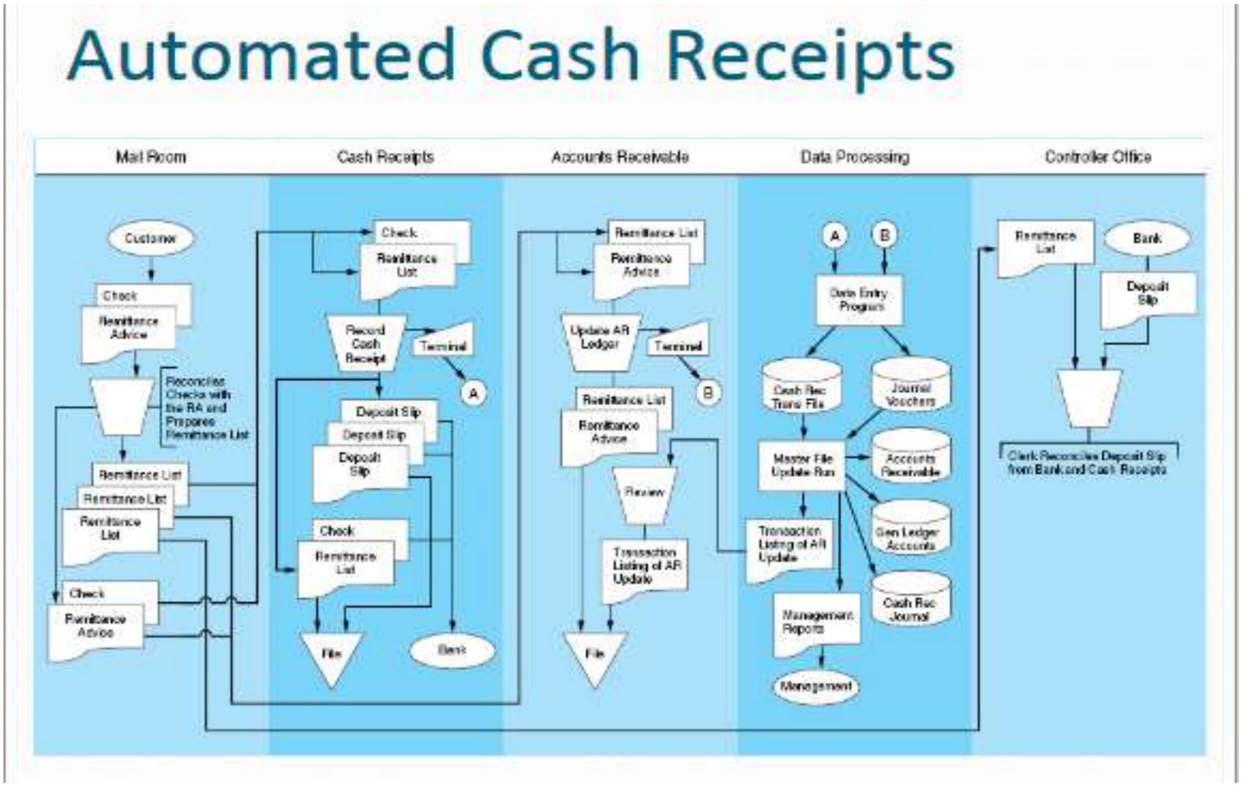
ii. Better inventory management which can lead to a competitive advantage.

iii. Fewer clerical errors, reducing incorrect items being shipped and bill discrepancies.

iv. Reduces the amount of expensive paper documents and their storage costs.

Reengineered Cash Receipts

- The mail room is a frequent target for reengineering.
- Companies send their customers preprinted envelopes and remittance advices.
- Upon receipt, these envelopes are scanned to provides a control procedure against theft.
- Machines are open the envelopes, scan remittance advices and checks, and separate the checks.
- Artificial intelligence may be used to read handwriting, such as remittance amounts and signatures.



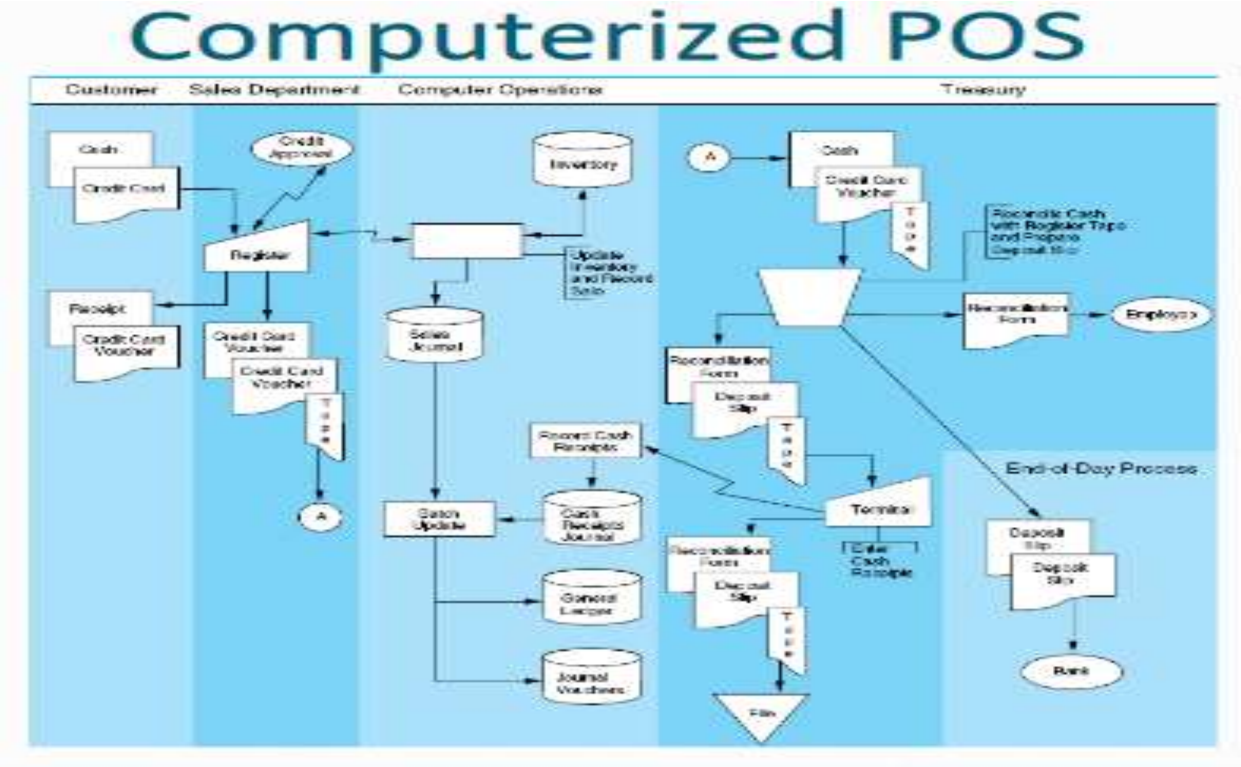
Automated Cash Receipts

Point-of-Sale Systems

- Point of sale systems are used extensively in retail establishments.
  - Customers pick the inventory from the shelves and take them to a cashier.
- The clerk scans the universal product code (UPC). The POS system is connected to an inventory file, where the price and description are retrieved.
  - The inventory levels are updated and reorder needs can immediately be detected.

Point-of-Sale Systems

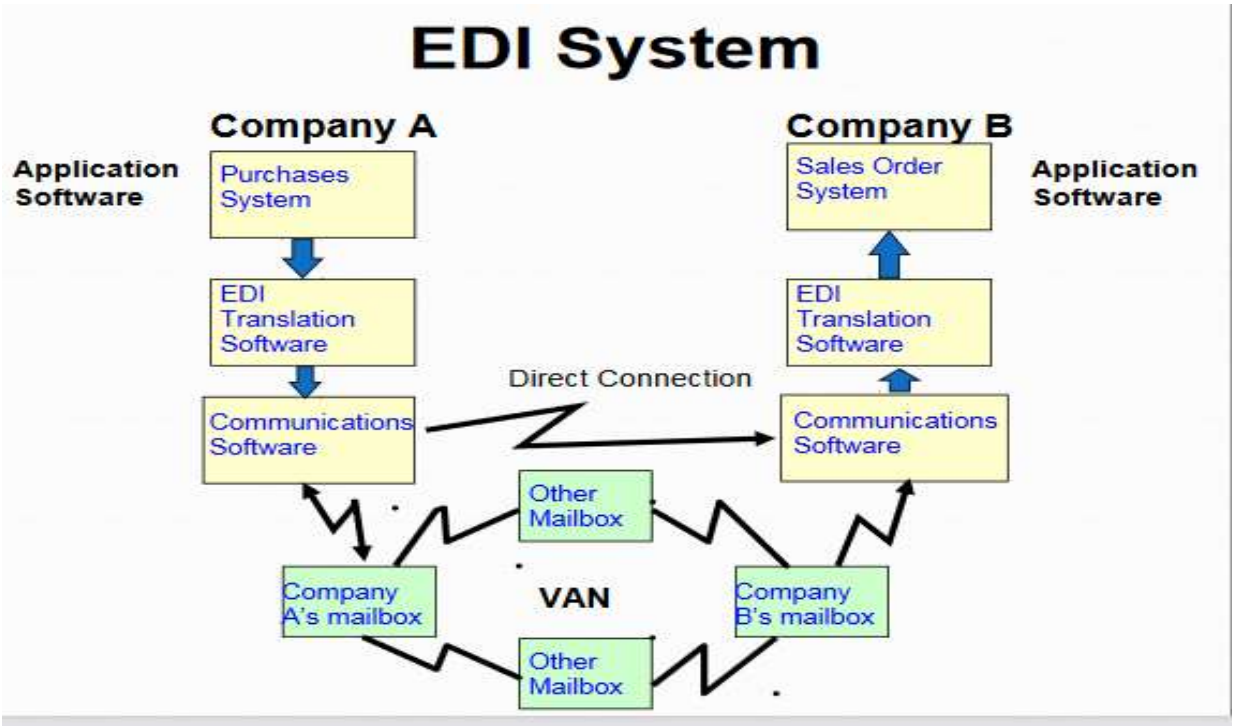
- The system computes the amount due. Payment is either cash, check, ATM or credit card in most cases.
  - No accounts receivables
- If checks, ATM or credit cards are used, an on-line link to receive approval is necessary.
- At the end of the day or a cashier’s shift, the money and receipts in the drawer are reconciled to the internal cash register tape or a printout from the computer’s database.
  - Cash over and under must be recorded



Computerized POS

Reengineering Using EDI

- EDI helps to expedite transactions.
- The customer's computer:
  - determines that inventory is needed
  - selects a supplier with whom the business has a formal business agreement
  - dials the supplier's computer and places the order
- The exchange is completely automated.
  - No human intervention or management



Reengineering Using the Internet

- Typically, no formal business agreements exist as they do in EDI.
- Most orders are made with credit cards.
- Mainly done with e-mail systems, and thus a turnaround time is necessary
  - Intelligent agents are needed to eliminate this time lag.
- Security and control over data is a concern with Internet transactions.

CBAS Control Considerations

- Authorization - in real-time systems, authorizations are automated
  - Programmed decision rules must be closely monitored.
- Segregation of Functions - consolidation of tasks by the computer is common
  - Protect the computer programs
  - Coding, processing, and maintenance should be separated.
- Supervision - in POS systems, the cash register's internal tape or database is an added form of supervision
- Access Control - magnetic records are vulnerable to both authorized and unauthorized exposure and should be protected
  - Must have limited file accessibility

  - Must safeguard and monitor computer programs
- Accounting Records - rest on reliability and security of stored digitalized data
  - Accountants should be skeptical about the accuracy of hard-copy printouts.
  - Backups -the system needs to ensure that backups of all files are continuously kept
- Independent Verification – consolidating accounting tasks under one computer program can remove traditional independent verification controls. To counter this problem:
  - perform batch control balancing after each run
  - produce management reports and summaries for end users to review

PC-Based Accounting Systems

- Used by small firms and some large decentralized firms
- Allow one or few individuals to perform entire accounting function
- Most systems are divided into modules controlled by a menu-driven program:
  - general ledger
  - inventory control
  - payroll
  - cash disbursements
  - purchases and accounts payable
  - cash receipts
  - sales order

PC Control Issues

- Segregation of Duties - tend to be inadequate and should be compensated for with increased supervision, detailed management reports, and frequent independent verification
- Access Control - access controls to the data stored on the computer tends to be weak; methods such as encryption and disk locking devices should be used
- Accounting Records - computer disk failures cause data losses; external backup methods need to be implemented to allow data recovery

4.7 THE EXPENDITURE CYCLE: PURCHASING AND CASH DISBURSEMENTS

4.7.1 Introduction

4.7.2 Study objectives:

i. To study the basic business activities and data processing operations that are performed in the expenditure cycle

ii. To study the decisions that needs to be made in the expenditure cycle, and what information is needed to make these decisions

iii. To study the major threats in the expenditure cycle and the controls related to those threats.

The primary external exchange of information is with suppliers (vendors). Information flows to the expenditure cycle from other cycles, e.g.:–*The revenue cycle, production cycle, inventory control, and various departments provide information about the need to purchase goods and materials*. Information also flows from the expenditure cycle:–*When the goods and materials arrive, the expenditure cycle provides information about their receipt to the parties that have requested them*. *Information is provided to the general ledger and reporting function for internal and external financial reporting.*

The primary objective of the expenditure cycle is to minimize the total cost of acquiring and maintaining inventory, supplies, and services. Decisions that must be made include:

- What level of inventory and supplies should we carry?
- What vendors provide the best price and quality?
- Where should we store the goods?
- Can we consolidate purchases across units?
- How can IT improve inbound logistics?
- Is there enough cash to take advantage of early payment discounts?
- How can we manage payments to maximize cash flow?

Management also has to evaluate the efficiency and effectiveness of expenditure cycle processes. These evaluations require data about: *Events that occur, Resources affected*, *Agents who participate.* This data needs to be accurate, reliable, and timely.

The study looks at how the three basic AIS functions are carried out in the expenditure cycle: i.e;

– How do we capture and process data?
– How do we store and organize the data for decisions?
– How do we provide controls to safeguard resources (including data)?

4.8 EXPENDITURE CYCLE BUSINESS ACTIVITIES

The three basic activities performed in the expenditure cycle are:

1. **Ordering goods, supplies, and services**
2. **Receiving and storing these items**
3. **Paying for these items**

These activities mirror the activities in the revenue cycle. let us discuss them one by one below.

1. ORDERING GOODS, SUPPLIES, AND SERVICES

Key decisions in this process involve identifying what, when, and how much to purchase and from whom. Weaknesses in inventory control can create significant problems with this process: *Inaccurate records cause shortages.* One of the key factors affecting this process is the inventory control method to be used.

Alternate Inventory Control Methods:

a. Economic Order Quantity (EOQ)

b. Just in Time Inventory (JIT)

c. Materials Requirements Planning (MRP)

Economic Order Quantity (EOQ)

EOQ is the traditional approach to managing inventory.

- Goal: Maintain enough stock so that production doesn't get interrupted.
- Under this approach, an optimal order size is calculated by minimizing the sum of several costs:
  - ➢ Ordering costs,
  - ➢ Carrying costs,
  - ➢ Stockout costs.
- The EOQ formula is also used to calculate reorder point, i.e., the inventory level at which a new order should be placed.
- Other, more recent approaches try to minimize or eliminate the amount of inventory carried.

Materials Requirements Planning (MRP)

MRP seeks to reduce inventory levels by improving the accuracy of forecasting techniques and carefully scheduling production and purchasing around that forecast.

Just in time inventory (JIT)

JIT systems attempt to minimize or eliminate inventory by purchasing or producing only in response to actual (as opposed to forecasted) sales. These systems have frequent, small deliveries of materials, parts, and supplies directly to the location where production will occur. A factory with a JIT system will have multiple receiving docks for their various work centers.

Similarities and differences between MRP and JIT:

a. Scheduling production and inventory accumulation

➢ MRP schedules production to meet estimated sales and creates a stock of finished goods inventory to be available for those sales. JIT schedules production in response to actual sales and virtually eliminates finished goods inventory, because goods are sold before they're made.

b. Nature of products

- MRP systems are better suited for products that have predictable demand, such as consumer staples. JIT systems are particularly suited for products with relatively short life cycles (e.g., fashion items) and for which demand is difficult to predict.

c. **Costs and efficiency**

- Both can reduce costs and improve efficiency over traditional EOQ approaches.

d. **Too much or too little**

- In either case, you must be able to: Quickly accelerate production if there is unanticipated demand and Quickly stop production if too much inventory is accumulating. Whatever the inventory control system, the order processing typically begins with a purchase request followed by the generation of a purchase order. *A request to purchase goods or supplies is triggered by either: The inventory control function; or An employee noticing a shortage.*
- Advanced inventory control systems automatically initiate purchase requests when quantity falls below the reorder point.

The need to purchase goods typically results in the creation of a purchase requisition. The purchase requisition is a paper document or electronic form that identifies:

- Who is requesting the goods
- Where they should be delivered
- When they're needed
- Item numbers, descriptions, quantities, and prices
- Possibly a suggested supplier
- Department number and account number to be charged

Most of the detail on the suppliers and the items purchased can be pulled from the supplier and inventory master files. The purchase requisition is received by a purchasing agent (aka, buyer) in the purchasing department, who typically performs the purchasing activity. In manufacturing companies, this function usually reports to the VP of Manufacturing.

A crucial decision is the selection of supplier. Key considerations are:–

- Price
- Quality
- Dependability
  - Especially important in JIT systems because late or defective deliveries can bring the whole system to a halt.
  - Consequently, certification that suppliers meet ISO 9000 quality standards is important. This certification recognizes that the supplier has adequate quality control processes.

Once a supplier has been selected for a product, their identity should become part of the product inventory master file so that the selection process does not have to be carried out for every purchase.

- A list of potential alternates should also be maintained. For products that are seldom ordered, the selection process may be repeated every time

It's important to track and periodically evaluate supplier performance, including data on: *Purchase prices, Rework and scrap costs, Supplier delivery performance*

The purchasing function should be evaluated and rewarded based on how well it minimizes total costs, not just the costs of purchasing the goods.

A ***purchase order*** is a document or electronic form that formally requests a supplier to sell and deliver specified products at specified prices. The PO is both a contract and a promise to pay. It includes:

- Names of supplier and purchasing agent
- Order and requested delivery dates
- Delivery location
- Shipping method
- Details of the items ordered

Multiple purchase orders may be completed for one purchase requisition if multiple vendors will fill the request. The ordered quantity may also differ from the requested quantity to take advantage of quantity discounts. A blanket order is a commitment to buy specified items at specified prices from a particular supplier for a set time period.

- Reduces buyer's uncertainty about reliable material sources
- Helps supplier plan capacity and operations

IT can help improve efficiency and effectiveness of purchasing function. The major cost driver is the number of purchase orders processed. Time and cost can be cut by:

4.9 Using EDI to transmit purchase orders

In a vendor managed inventory systems (VMIs):

- Inventory control and purchasing are outsourced to a supplier
- The supplier has access to PSO and inventory data and automatically replenishes inventory
- This approach: reduces amount of inventory carried, and eliminates costs of generating purchase orders
- Requires good controls to ensure accuracy of inventory records

Reverse auctions

Suppliers compete with each other to meet demand at the lowest price. Best suited to commodities, rather than critical components, where quality, vendor reliability, and delivery performance are not crucial

Pre-award audits

Used for large purchases that involve formal bids. Internal auditor visits each potential supplier in final cut to verify accuracy of their bid. May identify mathematical errors in bid which can produce considerable savings

Procurement cards for small purchases

A corporate credit card can be used with specific suppliers for specific types of purchases. Spending limits can be set. Account numbers on cards can be mapped to general ledger accounts

2. RECEIVING AND STORING GOODS

The receiving department accepts deliveries from suppliers.–Normally reports to warehouse manager, who reports to VP of Manufacturing. Inventory stores typically stores the goods. *Also reports to warehouse manager*. The receipt of goods must be communicated to the inventory control function to update inventory records. The two major responsibilities of the receiving department are: *Deciding whether to accept delivery and Verifying the quantity and quality of delivered goods*

The first decision is based on whether there is a valid purchase order. *Accepting un-ordered goods wastes time, handling and storage.*

Verifying the quantity of delivered goods is important so: The company only pays for goods received and Inventory records are updated accurately.

The ***receiving report*** is the primary document used in this process:

- It documents the date goods received, shipper, supplier, and PO number
- Shows item number, description, unit of measure, and quantity for each item
- Provides space for signature and comments by the person who received and inspected

Receipt of services is typically documented by supervisory approval of the supplier’s invoice.

When goods arrive, a receiving clerk compares the PO number on the packing slip with the open PO file to verify the goods were ordered.

- Then counts the goods
- Examines for damage before routing to warehouse or factory

Three possible exceptions in this process:

- The quantity of goods is different from the amount ordered
- The goods are damaged
- The goods are of inferior quality

If one of these exceptions occurs, the purchasing agent resolves the situation with the supplier.

- Supplier typically allows adjustment to the invoice for quantity discrepancies.

- If goods are damaged or inferior, a debit memo is prepared after the supplier agrees to accept a return or grant a discount.
    - One copy goes to supplier, who returns a credit memo in acknowledgment.
    - One copy to accounts payable to adjust the account payable.
    - One copy to shipping to be returned to supplier with the actual goods.

IT can help improve the efficiency and effectiveness of the receiving activity:

Bar-coding

Requiring suppliers to bar-code products speeds the counting process and improves accuracy.

RFID

Passive radio frequency identification (RFID) tags eliminate the need to scan bar codes.

EDI and satellite technology

EDI and satellite technology make it possible to track the exact location of incoming shipments and have receiving staff on hand to unload trucks. Also enables drivers to be directed to specific loading docks where goods will be used.

Audits

Audits can identify opportunities to cut freight costs and can ensure that suppliers are not billing for transportation costs they are supposed to assume.

3. PAYING FOR GOODS AND SERVICES

There are two basic sub-processes involved in the payment process:

i. Approval of vendor invoices;

ii. Actual payment of the invoices

i. Approval of vendor invoices

Approval of vendor invoices is done by the accounts payable department, which reports to the controller. The legal obligation to pay arises when goods are received.

- But most companies pay only after receiving and approving the invoice.
- This timing difference may necessitate adjusting entries at the end of a fiscal period.

Objective of accounts payable:

- Authorize payment only for goods and services that were ordered and actually received. Requires information from: **Purchasing** — *about existence of valid purchase order*. **Receiving** — *for receiving report indicating goods were received*

There are two basic approaches to processing vendor invoices:

a. **Non-voucher system**

- Each invoice is stored in an open invoice file.
- When a check is written, the invoice is marked "paid" and then stored in a paid invoice file.

b. **Voucher system**

A disbursement voucher is prepared which lists: *Outstanding invoices for the supplier and Net amount to be paid after discounts and allowances.*

The disbursement voucher effectively shows which accounts will be debited and credited, along with the account numbers.

Advantages of a voucher system:

Several invoices may be paid at once, which reduces number of checks written. Vouchers can be pre-numbered which simplifies the audit trail for payables. Invoice approval is separated from invoice payment, which makes it easier to schedule both to maximize efficiency.

There are two basic sub-processes involved in the payment process:

1) Approval of vendor invoices
2) Actual payment of the invoices

1. Actual payment of the invoices

Payment of the invoices is done by the cashier, who reports to the treasurer. The cashier receives a voucher package, which consists of the vendor invoice and supporting documentation, such as purchase order and receiving report. This voucher package authorizes issuance of a check or EFT to the supplier.

Referred to as Evaluated Receipt Settlement. Payments are issued based on what is ordered and received. Requires that:

- Suppliers quote accurate prices when orders are placed.
- Receiving personnel count accurately and inspect merchandise received.

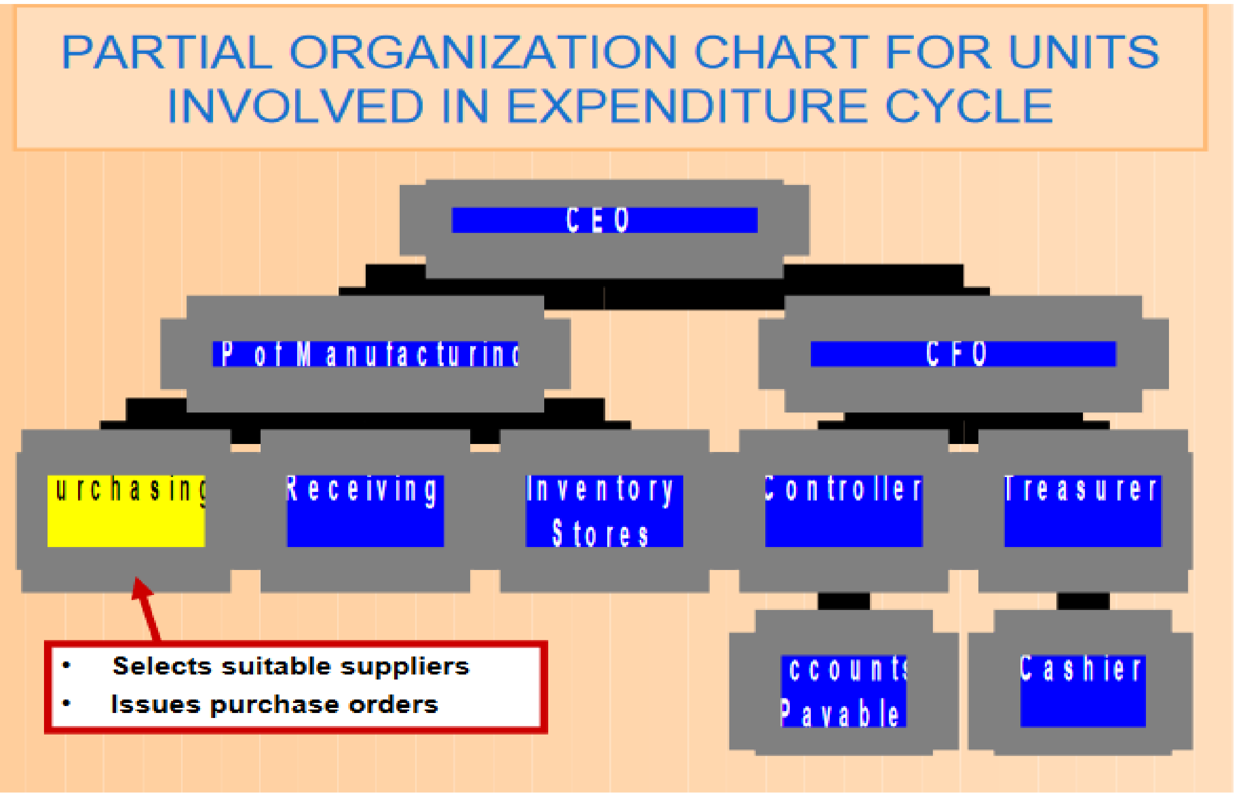
Typically incorporates very timely communications about shipments and receipts.

Processing efficiency can be improved by:

- Requiring suppliers to submit invoices by EDI
- Having the system automatically match invoices to POs and receiving reports
- Eliminating vendor invoices
- Using procurement cards for non-inventory purchases
- Using company credit cards and electronic forms for travel expenses.
- Preparing careful cash budgets to take advantage of early-payment discounts.
- Using FEDI to pay suppliers

4.10 REVIEW OF EXPENDITURE CYCLE ACTIVITIES

Before we move on to discuss internal controls in the expenditure cycle, let’s do a brief review of the organization chart, including: *Who does what in the expenditure cycle and To whom they typically report.*



PARTIAL ORGANIZATION CHART FOR UNITS INVOLVED IN EXPENDITURE CYCLE

CEO

P of Manufacturinc

CFO

urchasing

Receiving

Inventory Stores

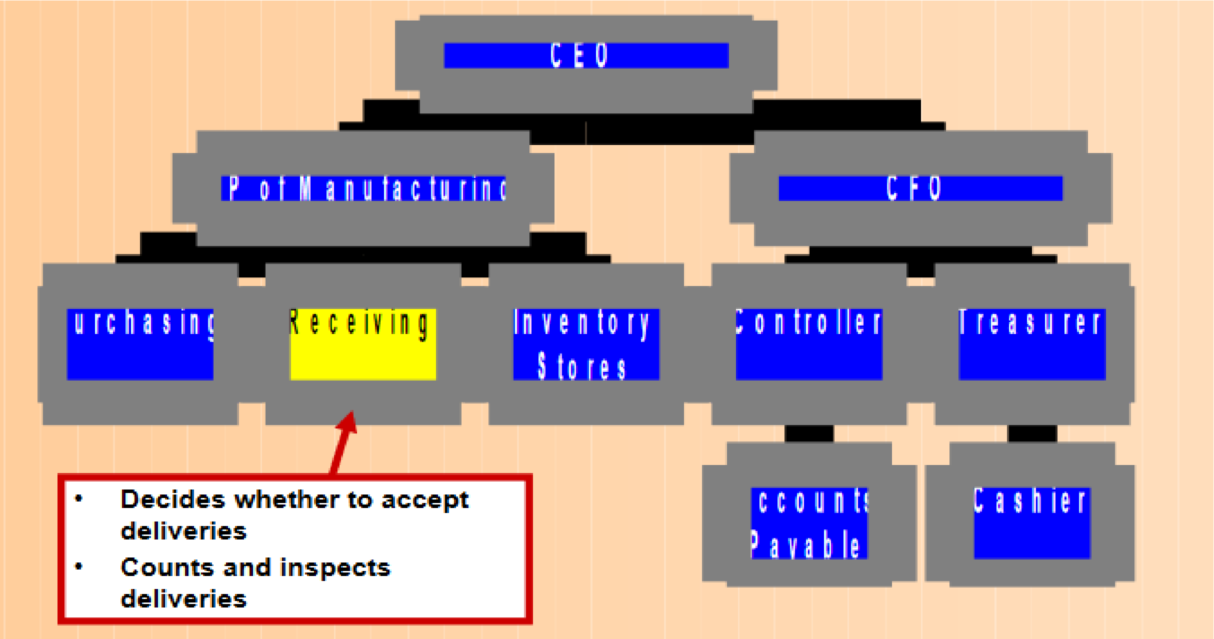
Controller

Treasurer

ccounts Payable

Cashier

- Selects suitable suppliers
- Issues purchase orders



CEO

P of Manufacturinc

CFO

urchasing

Receiving

Inventory Stores

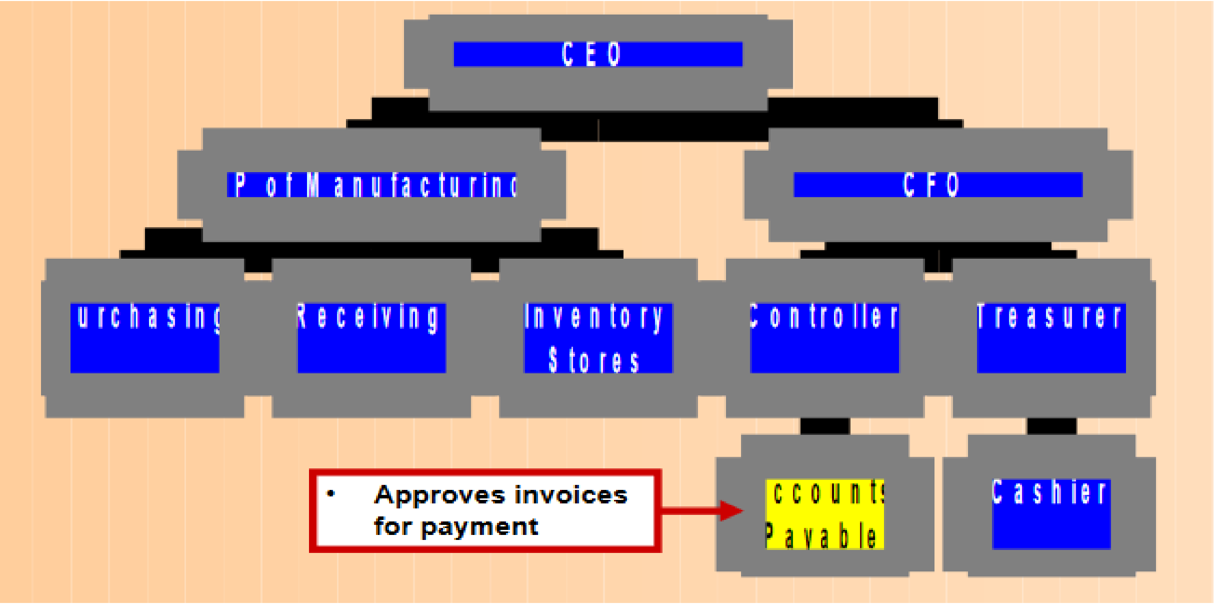
Controller

Treasurer

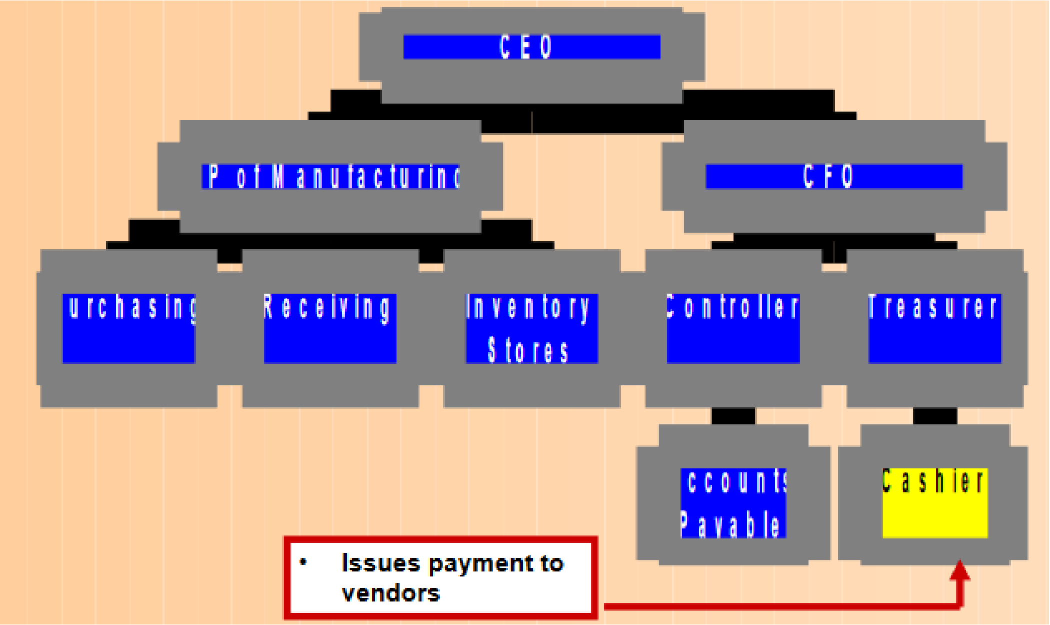
ccounts Payable

Cashier

- Decides whether to accept deliveries
- Counts and inspects deliveries



- Approves invoices for payment



- Issues payment to vendors

4.11 CONTROL: OBJECTIVES, THREATS, AND PROCEDURES

In the expenditure cycle (or any cycle), a well-designed AIS should provide adequate controls to ensure that the following objectives are met:

- All transactions are properly authorized
- All recorded transactions are valid
- All valid and authorized transactions are recorded
- All transactions are recorded accurately
- Assets are safeguarded from loss or theft

- Business activities are performed efficiently and effectively
- The company is in compliance with all applicable laws and regulations
- All disclosures are full and fair.

There are several actions a company can take with respect to any cycle to reduce threats of errors or irregularities. These include:

- Using simple, easy-to-complete documents with clear instructions (enhances accuracy and reliability).
- Using appropriate application controls, such as validity checks and field checks (enhances accuracy and reliability).
- Providing space on forms to record who completed and who reviewed the form (encourages proper authorizations and accountability).
- Pre-numbering documents (encourages recording of valid and only valid transactions).
- Restricting access to blank documents (reduces risk of unauthorized transaction).

In the following sections, we'll discuss the threats that may arise in the three major steps of the expenditure cycle, as well as general threats, EDI-related threats, and threats related to purchases of services.

Before we discuss specific threats, it may be helpful to have some background on a form of occupational fraud and abuse which is broadly referred to as corruption. Corruption cases often involve arrangements between a company's purchasing agent and a sales representative for one of the company's vendors.

4.12 CRIME TIME

The vendor's representative may try to induce the purchasing agent to buy goods that:

- Are over-priced
- Are of inferior quality
- Aren't even needed
- Aren't even delivered

In exchange, the vendor's rep typically offers the purchasing agent something of value. That "something" might be money, payment of a debt, a job offer, an expensive vacation, or anything the purchasing agent might value.

According to the *Fraud Examiner's Manual* published by the Association of Certified Fraud Examiners, these schemes usually take four forms:

Bribery

- Typically involves the vendor offering a kickback(something of value) to the buyer to buy inflated, substandard, un-needed, or un-delivered goods, etc.
- Alternately, may involve an inducement to the buyer to rig a competitive bidding process so that the vendor gets the bid.

Conflict of interest

- In conflict of interest cases, the purchasing agent is usually arranging for his employer to make purchases from a company in which he has a concealed interest.

- For example, perhaps his wife owns the vendor company.

Economic extortion

- Economic extortion is basically the reverse of a bribe.
- Instead of the vendor making an offer of something of value to the purchasing agent, the purchasing agent may tell the vendor that he must provide something of value to the purchasing agent if he wants to continue to do business with his employer.

Illegal gratuities

- Illegal gratuities involve gifts that are given to the purchasing agent by a vendor after the vendor has been selected.
- There was no intent by the vendor to influence the selection process; the gift was provided after the fact.
- But the problem is that the gift is too likely to impact future decisions by the purchasing agent.

Threats in the process of ordering goods include:

- **THREAT** 1: Stockouts and/or Excess Inventory
- **THREAT 2**: Ordering Unnecessary Items
- **THREAT 3**: Purchasing Goods at Inflated Prices
- **THREAT 4**: Purchasing Goods of Inferior Quality
- **THREAT 5:** Purchasing from Unauthorized Suppliers
- **THREAT 6**: Kickbacks
- EDI-Related Threats
- Threats Related to Purchases of Services

THREAT NO. 1—STOCKOUTS AND/OR EXCESS INVENTORY

Why is this a problem?

- If you run out of merchandise, you may lose sales
- If you carry too much merchandise, you incur excess carrying costs and/or have to mark the inventory down.

Controls:

- Accurate inventory control and sales forecasting systems
- Use of the perpetual inventory method

Supplier performance reports that highlight deviations in product quality, price, and on-time delivery. Online accounting information systems to record changes to inventory in real time. Bar-coding of inventory to improve accuracy. Periodic physical counts of inventory to verify accuracy of the records.

THREAT NO. 2—ORDERING UNNECESSARY ITEMS

Why is this a problem?

- Excess carrying costs
- Obsolete inventory that can't be sold or has to be marked down

A related problem is multiple purchases of the same item by different units of the organization

- Often occurs when different departments or divisions have different numbering systems for parts
- Causes company to miss out on volume discounts

Controls:

- Design the AIS to integrate the databases of various units
- Produce reports that link item descriptions to part numbers.

THREAT NO. 3—PURCHASING GOODS AT INFLATED PRICES

Why is this a problem?

- Increases product costs
- Reduces profitability and/or damages competitive position

Controls:

- Price lists for frequently purchased items—stored in master file and consulted
- Prices of low-cost items determined from catalogs.
- Bids should be solicited for high-cost and specialized products
- Purchase orders should be reviewed to be sure policies have been followed
- Budgetary controls and responsibility accounting should be utilized to achieve accountability for cost overruns
- Performance reports should highlight significant variances for investigation.

THREAT NO. 4—PURCHASING GOODS OF INFERIOR QUALITY

Why is this a problem?

- Can result in costly production delays
- Scrap and rework costs may make these materials more expensive than high-quality alternatives

Controls:

- Compile list of approved suppliers known to provide goods of acceptable quality.
- Review purchase orders to ensure use of approved suppliers.
- Track and review supplier performance
- Hold purchasing managers responsible for the total cost of purchases, including rework and scrap costs
    - Requires that the AIS can track these costs.

THREAT NO. 5—PURCHASING FROM UNAUTHORIZED SUPPLIERS

Why is this a problem?

- May result in goods of inferior quality
- May cause legal issues such as violation of import quotas

Controls:

- Review purchase orders for use of approved suppliers
- Restrict access to approved supplier list

Periodically review approved supplier list for unauthorized changes. Work with issuers of procurement cards to control which suppliers can accept the card.

THREAT NO. 6—KICKBACKS

Why is this a problem?

- Kickbacks are gifts from suppliers to purchasing agents for the purpose of influencing their choice of suppliers. They typically result in many of the preceding threats, including:
  - Paying inflated prices
  - Buying unneeded items
  - Buying goods of inferior quality

Controls:

- Prohibit purchasing agents from accepting gifts from suppliers.
- Train employees to respond appropriately to gifts from suppliers.
- Rotate jobs so the same purchasing agent does not deal with the same suppliers indefinitely.
- Audit the activities of purchasing agents.
- Enforce mandatory vacations.
- Have purchasing agents review and sign annual conflict of interest statements.
- Include clauses allowing vendor audits in contracts with suppliers.

EDI-RELATED THREATS

Why is this a problem?

- Users who have malicious intent and/or have unauthorized access to EDI can submit multiple unauthorized transactions quickly.

Controls:

- Access to the EDI system should be limited to authorized personnel through passwords, user IDs, access control matrices, and physical access controls.
- Procedures should be in place to verify and authenticate EDI transactions
- EDI systems should send an acknowledgment for each transaction:
  - Provides an accuracy check
  - Helps protect against transmission problems that could result in loss of an order
- A log of all EDI transactions should be maintained and reviewed by an independent party
- Encryption should be used to ensure privacy, particularly for competitive bids
- Digital signatures should be used to ensure authenticity
- Companies should have agreements with suppliers over EDI-related concerns.

THREATS RELATED TO PURCHASES OF SERVICES

Why is this a problem?

- Services are not a physical product and can't be counted. It can be difficult to "audit" whether they were provided.

Controls:

- Hold supervisors responsible for all costs incurred by their departments.
- Compare actual vs. budgeted expenses, and investigate discrepancies.
- Conduct periodic reviews of contracts for services, including audits of supplier records

THREATS IN RECEIVING AND STORING GOODS

The primary objectives of this process are to:

- Verify the receipt of ordered inventory
- Safeguard the inventory against loss or theft.

Threats in the process of receiving and storing goods include:

- **THREAT 7: Receiving unordered goods**
- THREAT 8: Errors in counting received goods
- THREAT 9: Theft of inventory

THREAT NO. 7—RECEIVING UNORDERED GOODS

Why is this a problem?

- Results in unnecessary costs to unload, store, and return the items

Controls:

- Instruct receiving department to accept goods only if there is an approved copy of the purchase order.

THREAT NO. 8—ERRORS IN COUNTING RECEIVED GOODS

Why is this a problem?

- Company pays for goods that weren’t received
- Inventory records are inaccurate, possibly leading to stockouts and lost sales

Controls:

- Bar coding of ordered goods
- Design receiving forms so clerks cannot see the quantity ordered
- Require receiving clerks to sign receiving reports to create accountability.
- Offer bonuses for catching discrepancies
- Have inventory control count the items transferred from receiving

THREAT NO. 9—THEFT OF INVENTORY

Why is this a problem?

- Loss of assets
- Inaccurate records

Controls:

- Store inventory in secure locations with restricted access
- Document all intra-company inventory transfers, e.g.:
  - Goods moving from receiving to warehouse

  - Goods moving from warehouse to production floor

- Periodic physical count of inventory and comparison to records
- – More critical items should be counted more frequently
- Segregation of duties
- – Separate those who have physical access to inventory from those who keep records
- – Separate both those who have custody and those who can authorize inventory adjustments from those who work in the receiving and shipping functions.

THREATS IN THE PROCESS OF APPROVING AND PAYING VENDOR INVOICES

The primary objectives of this process are to:

- Pay only for goods and services that were ordered and received
- Safeguard cash

Threats in the process of approving and paying vendor invoices include:

- THREAT 10: Failing to catch errors in vendor invoices
- THREAT 11: Paying for goods not received
- THREAT 12: Failing to take available purchase discounts
- THREAT 13: Paying the same invoice twice
- THREAT 14: Recording and posting errors to accounts payable
- THREAT 15: Misappropriating cash, checks, or EFTs

THREAT NO. 10: Failing to Catch Errors in Vendor Invoices

Why is this a problem?

- Overpaying for merchandise

Controls:

- Check mathematical accuracy of invoices
- Obtain receipts from procurement card users and verify monthly statement accuracy
- Adopt Evaluated Receipt Settlement (ERS) approach—i.e., pay for goods when received at the price stated in the purchase order
- Freight-related terminology can be challenging, so provide accounts payable staff with training on transportation practices and terminology
- When freight is paid by the purchaser, use the same carrier in order to receive discounts

THREAT NO. 11: Paying for Goods Not Received

Why is this a problem?

- Increased costs

Controls:

- Compare quantities on invoice with quantities reported by receiving and inventory control departments

- Use ERS
- With respect to services, have tight budgetary controls and provide careful review of departmental expenses.

THREAT NO. 12: Failing to Take Available Purchase Discounts
Why is this a problem?

- Reduces profitability

Controls:

- File approved invoices by due date and track that way
- Prepare cash flow budgets to determine whether the company has adequate cash flow to take advantage of early payment discounts.

THREAT NO. 13: Paying the Same Invoice Twice
Why is this a problem?

- Reduces profitability
- Can create a cash crunch if a large invoice is paid twice

Controls:

- Approve invoices for payment only when accompanied by a complete voucher package (PO & receiving report)
- Only pay on original copies of invoices
- Cancel the invoice once the check is signed
- Have internal auditors or consultants help detect and recover overpayments
- In invoice-less accounts payable systems, control access to the master file and monitor all changes

THREAT NO. 14: Recording and Posting Errors to Accounts Payable
Why is this a problem?

- May result in disgruntled suppliers
- Causes errors in financial and performance reports

Controls:

- Appropriate data entry and processing controls, such as comparing the differences in vendor balances before and after processing checks with the total amount of invoices processed
- Reconcile supplier balances (or unpaid vouchers) with the accounts payable control account

THREAT NO. 15: Misappropriating Cash, Checks, or EFTs
Why is this a problem?

- Loss of assets
- Potentially misleading financial statements if theft is large enough

Controls:

- Restrict access to cash, blank checks, and check signing machines
- Have checks numbered sequentially and periodically accounted for by the cashier.

- To prevent schemes where an employees causes his employer to issue a fraudulent check:
- Use proper segregation of duties: »Accounts payable authorizes payment» The treasurer or cashier signs and mails checks
- Require two signatures for checks over a certain amount
- Restrict access to the approved supplier list; have changes reviewed and approved
- Cancel all documents in the voucher package when payment is made
- Have an independent party (e.g., internal auditing) reconcile the bank statements.

To prevent check alteration and forgery:

- Use check protection machines that imprint amounts
- Use inks that are difficult to alter
- Print checks on watermarked paper
- Set up a positive pay arrangement with the bank

  » The company provides the bank with a list of checks it has written
  » The bank will only honor checks that are on that list
- Do bank reconciliations promptly

If a petty cash fund is needed:

- It should be handled by an employee who has no other cash-handling or accounting responsibilities
- It should be set up as an imprest fund (fixed amount that gets replenished on presentation of vouchers)
- Vouchers should be canceled when the fund is replenished
- Periodic surprise counts should be made and the custodian should be held responsible for shortages.

Electronic funds transfer requires additional control procedures, including:

- Strict physical and logical access controls
- Change password and user IDs regularly
- Log user and location of originating terminal
- Transactions should be encrypted
- Transactions should be time stamped and numbered
- A control group should monitor the transactions and the EFT controls
- Embedded audit modules can be incorporated to electronically monitor the transactions and flag suspicious items.

GENERAL CONTROL ISSUES

THREAT NO. 16—LOSS, ALTERATION, OR UNAUTHORIZED DISCLOSURE OF DATA–Why is this a problem?

Loss or alteration of data could cause:

- Errors in external or internal reporting.
- Inaccurate payment of vendors

Unauthorized disclosure of confidential vendor information can cause:

- Legal sanctions and fines
- Vendor bidding irregularities

Controls:

- The purchases file, cash disbursements file, accounts payable master file, and most recent transaction file should be backed up regularly.
    - At least one backup on site and one offsite.
- All disks and tapes should have external and internal file labels to reduce chance of accidentally erasing important data.
- Access controls should be utilized:
    - User IDs and passwords
    - Compatibility matrices
    - Controls for individual terminals (e.g., so the sales order department can't create a receiving report)
    - Logs of all activities, particularly those requiring specific authorizations.
    - Default settings on ERP systems usually allow users far too much access to data, so these systems must be modified to enforce proper segregation of duties.
    - Sensitive data should be encrypted in storage and in transmission.
    - Parity checks, acknowledgment messages, and control totals should be used to ensure transmission accuracy.

THREAT NO. 17—POOR PERFORMANCE

Why is this a problem?

- May damage vendor relations
- Reduces profitability

Controls:

- Prepare and review performance reports

4.13 EXPENDITURE CYCLE INFORMATION NEEDS

Information is needed for the following operational tasks in the expenditure cycle, including:

- Deciding when and how much inventory to order
- Deciding on appropriate suppliers
- Determining if vendor invoices are accurate
- Deciding whether to take purchase discounts
- Determining whether adequate cash is available to meet current obligations

Information is also needed for the following strategic decisions:

- Setting prices for products/services

- Establishing policies on returns and warranties
- Deciding on credit terms
- Determining short-term borrowing needs
- Planning new marketing campaigns.

The AIS needs to provide information to evaluate the following:

- Purchasing efficiency and effectiveness
- Supplier performance
- Time taken to move goods from receiving to production
- Percent of purchase discounts taken

Both financial and operating information are needed to manage and evaluate these activities. Both external and internal information are needed.

When the AIS integrates information from the various cycles, sources, and types, the reports that can be generated are unlimited. They include reports on:

- Supplier performance
- Outstanding invoices
- Performance of expenditure cycle employees
- Number of POs processed by purchasing agent
- Number of invoices processed by A/P clerk
- Number of deliveries handled by receiving clerk
- Number of inventory moves by warehouse worker
- Inventory turnover
- Classification of inventory based on contribution to profitability

Accountants should continually refine and improve these performance reports

4.16 SUMMARY

- You’ve learned about the basic business activities and data processing operations that are performed in the expenditure cycle, including:
  - Ordering goods, supplies, and services
  - Receiving and storing them
  - Approving invoices and paying for them
- You’ve learned how IT can improve the efficiency and effectiveness of these processes.
- You’ve learned about decisions that need to be made in the expenditure cycle and what information is required to make these decisions
- You’ve also learned about the major threats that present themselves in the expenditure cycle and the controls that can mitigate those threats

Unit 5

5.0 FRAUD AND COMPUTER SECURITY

The unit shall help the candidates have diverse knowledge on how businesses can secure their information that is critical to their success. Hence the key protective methodologies are adopted to safeguard the company from the technological risks.

The study aims to achieve the following

i. What fraud is and how its perpetrated
ii. Perpetrators of fraud
iii. Forms of computer fraud
iv. Approaches used in committing these frauds

5.1 INTRODUCTION

Information systems are becoming increasingly more complex and society is becoming increasingly more dependent on these systems.– Companies also face a growing risk of these systems being compromised. Companies have suffered security breaches in almost every year leading to reporting financial losses. Apart from natural or terror activities that can generally affect business, we have heard or witnessed espionage agents, foreign companies targeted by other foreign countries in almost every year globally.

These intentional acts are the ones that lead to computer crimes. These include;

- ➢ Sabotage.
- ➢ Computer fraud.
- ➢ Misrepresentation, false use, or unauthorized disclosure of data.
- ➢ Misappropriation of assets,
- ➢ Financial statement fraud.

Information systems are increasingly vulnerable to these malicious attacks.

5.2 FRAUD:

What is Fraud?

Fraud is any intentional act or omission designed to deceive others to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain, usually, monetary.

Some Dictionary Definitions......

•“A deception deliberately practiced in order to secure unfair or unlawful gain” or

•“Deliberate deception or cheating intended to gain an illegal advantage” also we can say that it is;

–A false statement (oral or in writing)

–About a material fact

–Knowledge that the statement was false when it was uttered (which implies an intent to deceive)

–A victim relies on the statement

–And suffers injury or loss as a result

5.2.1 THE FRAUD PROCESS

Since fraudsters don’t make journal entries to record their frauds, we can only estimate the amount of losses caused by fraudulent acts:

- In 2004, the Association of Certified Fraud Examiners (ACFE) estimates that total fraud losses in the U.S. was around 6% of annual revenues or approximately $660 billion
- More than what USA spend on education and roads in a year.

- 6 times what they paid for the criminal justice system.
- Income tax fraud (the difference between what taxpayers owe and what they pay to the government) is estimated to be over $200 billion per year.
- Fraud in the healthcare industry was estimated to exceed $100 billion a year the same year.

Fraud against companies may be committed by an employee or an external party.

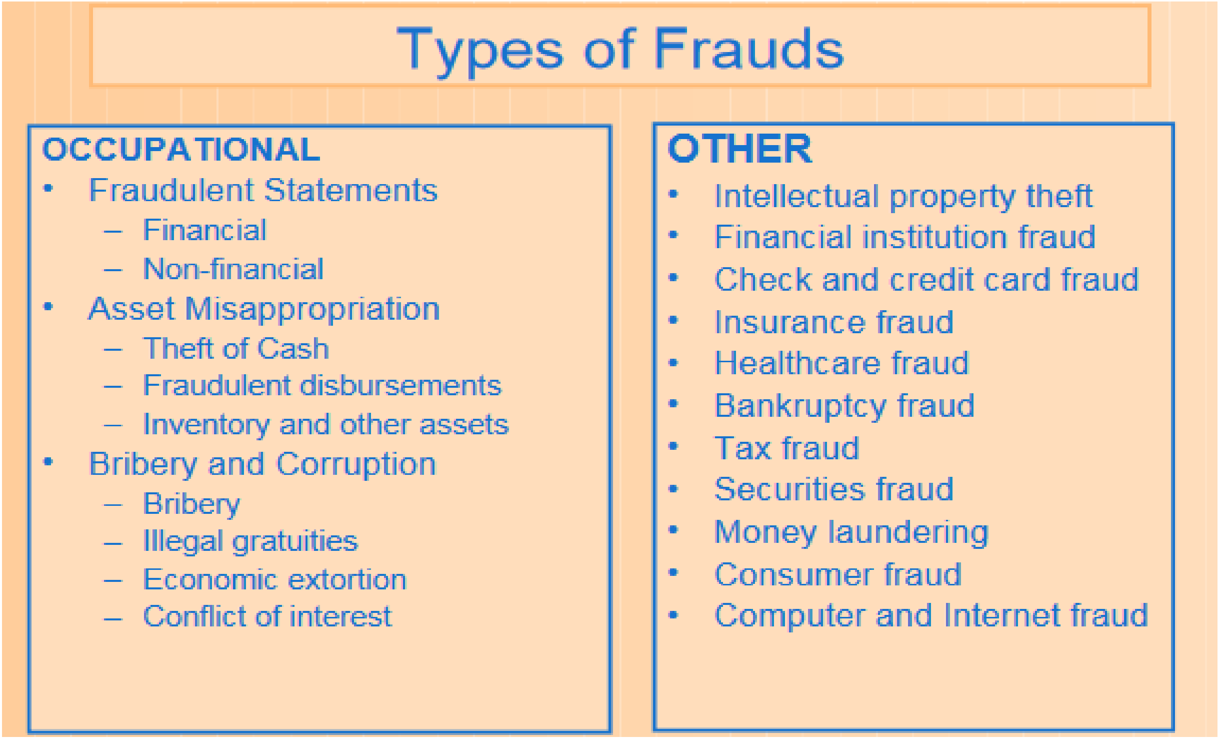
- Former and current employees (called knowledgeable insiders) are much more likely than non-employees to perpetrate frauds (and big ones) against companies.

  • *Largely owing to their understanding of the company's systems and its weaknesses, which enables them to commit the fraud and cover their tracks.*
- Organizations must utilize controls to make it difficult for both insiders and outsiders to steal from the company.

Fraud perpetrators are often referred to as *white-collar criminals*.

- ➢ Distinguishes them from violent criminals, although some white-collar crime can ultimately have violent outcomes, such as:
- Perpetrators or their victims committing suicide.
- Healthcare patients killed because of alteration of information, etc., that can result in their deaths.

5.2.2 Types of Fraud



Types of Frauds

OCCUPATIONAL

- Fraudulent Statements
  - Financial
  - Non-financial
- Asset Misappropriation
  - Theft of Cash
  - Fraudulent disbursements
  - Inventory and other assets
- Bribery and Corruption
  - Bribery
  - Illegal gratuities
  - Economic extortion
  - Conflict of interest

OTHER

- Intellectual property theft
- Financial institution fraud
- Check and credit card fraud
- Insurance fraud
- Healthcare fraud
- Bankruptcy fraud
- Tax fraud
- Securities fraud
- Money laundering
- Consumer fraud
- Computer and Internet fraud

Three types of occupational fraud:

1. Misappropriation of assets Involves ;

- ➢ Theft
- ➢ Embezzlement, or misuse of company assets for personal gain.•
  - ➢ Examples include billing schemes, check tampering, skimming, and theft of inventory.

2. Corruption

• Corruption involves the wrongful use of a position, contrary to the responsibilities of that position, to procure a benefit.

- ➢ Examples include kickback schemes and conflict of interest schemes.

3. Fraudulent statements
    - Financial statement fraud involves misstating the financial condition of an entity by intentionally misstating amounts or disclosures in order to deceive users.
    - Financial statements can be misstated as a result of intentional efforts to deceive or as a result of undetected asset misappropriations that are so large that they cause misstatement.

A typical employee fraud has a number of important elements or characteristics:–The fraud perpetrator must gain the trust or confidence of the person or company being defrauded in order to commit and conceal the fraud.

- Instead of using a gun, knife, or physical force, fraudsters use weapons of deceit and misinformation.
- Frauds tend to start as the result of a perceived need on the part of the employee and then escalate from need to greed. Most fraudsters can't stop once they get started, and their frauds grow in size.
- The fraudsters often grow careless or overconfident over time.
- Fraudsters tend to spend what they steal. Very few save it.
- In time, the sheer magnitude of the frauds may lead to detection.
- The most significant contributing factor in most employee frauds is the absence of internal controls and/or the failure to enforce existing controls.

The National Commission on Fraudulent Financial Reporting (aka, the Treadway Commission) defined fraudulent financial reporting as intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements.

Financial statements can be falsified to:

- ➢ Deceive investors and creditors
- ➢ Cause a company's stock price to rise
- ➢ Meet cash flow needs
- ➢ Hide company losses and problems

Fraudulent financial reporting is of great concern to independent auditors, because undetected frauds lead to half of the lawsuits against auditors.

In the case of Enron, a financial statement fraud led to the total elimination of Arthur Andersen, a premiere international public accounting firm.

Common approaches to "cooking the books" include:

- Recording fictitious revenues
- Recording revenues prematurely
- Recording expenses in later periods
- Overstating inventories or fixed assets (WorldCom)
- Concealing losses and liabilities

The Treadway Commission recommended four actions to reduce the possibility of fraudulent financial reporting:

- Establish an organizational environment that contributes to the integrity of the financial reporting process.
- Identify and understand the factors that lead to fraudulent financial reporting.
- Assess the risk of fraudulent financial reporting within the company.

- Design and implement internal controls to provide reasonable assurance that fraudulent financial reporting is prevented.

5.2.3 Why fraud occurs

Perpetrators of computer fraud tend to be younger and possess more computer knowledge, experience, and skills.

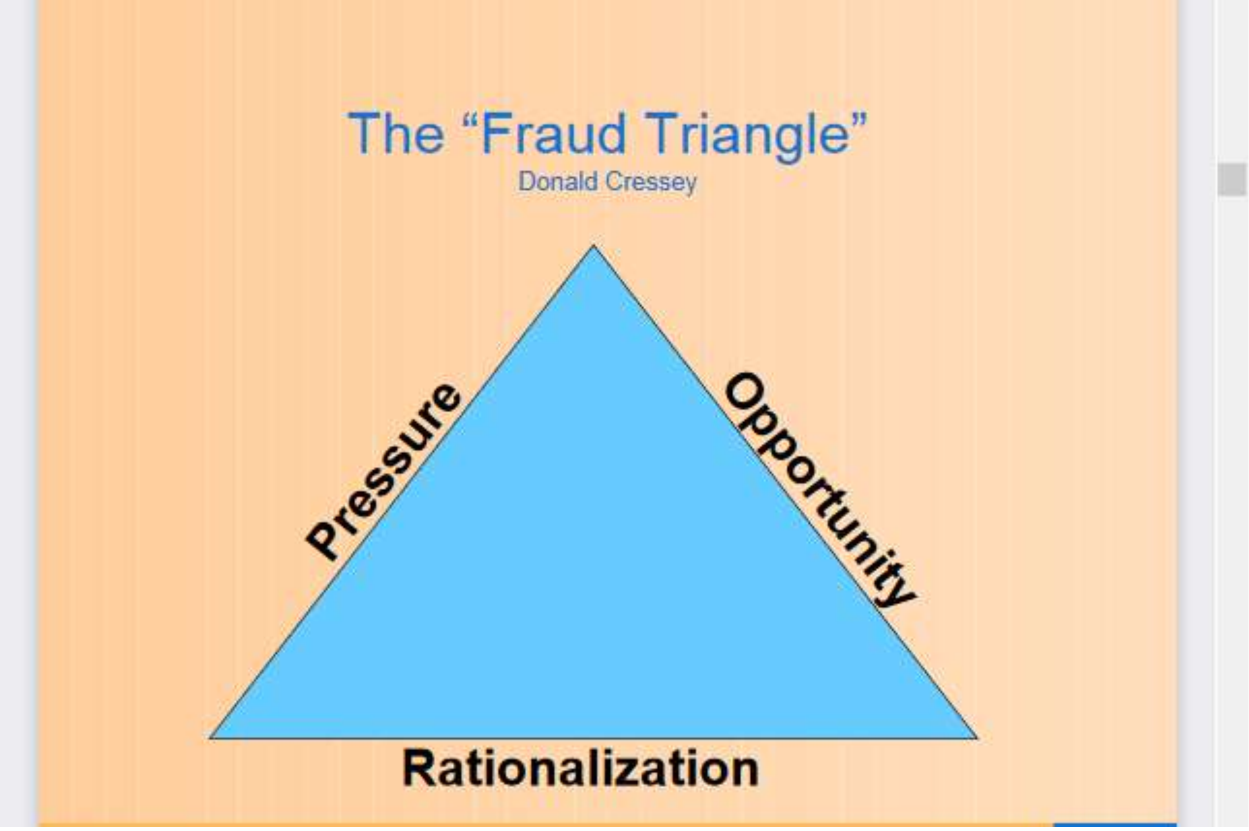
Hackers and computer fraud perps tend to be more motivated by:

- Curiosity
- A quest for knowledge
- The desire to learn how things work
- The challenge of beating the system
- They may view their actions as a game rather than dishonest behavior.
- Another motivation may be to gain stature in the hacking community.
- Some see themselves as revolutionaries spreading a message of anarchy and freedom.

But a growing number want to profit financially. To do so, they may sell data to:

- Spammers
- Organized crime
- Other hackers
- The intelligence community
- Some fraud perpetrators are disgruntled and unhappy with their jobs and are seeking revenge against their employers.
- Others are regarded as ideal, hard-working employees in positions of trust.
- Most have no prior criminal record.

So why are they willing to risk everything?



The "Fraud Triangle"

Donald Cressey

Pressure–

The pressure could be related to finances, emotions, lifestyle, or some combination.

There are many opportunities that enable fraud. Some of the most common are:

- Lack of internal controls
- Failure to enforce controls (the most prevalent reason)
- Excessive trust in key employees
- Incompetent supervisory personnel
- Inattention to details
- Inadequate staff

5.2.4 Opportunities permitting employee and financial statement fraud

- Internal Control Factors–
- Failure to enforce/monitor internal controls–
- Management not involved in control system–
- Management override of controls and guidelines–
- Managerial carelessness, inattention to details–
- Dominant and unchallenged management–
- Ineffective oversight by board of directors–
- No effective internal auditing staff–
- Infrequent third-party reviews–
- Insufficient separation of authorization, custody, and record-keeping duties–
- Too much trust in key employees–
- Inadequate supervision–
- Unclear lines of authority
- Lack of proper authorization procedures–
- No independent checks on performance–
- Inadequate documents and records–
- Inadequate system for safeguarding assets–
- No physical or logical security system–
- No audit trails–
- Failure to conduct background checks–
- No policy of annual vacations, rotation of duties

Creators of worms and viruses often use rationalizations like:

- The malicious code helped expose security flaws, so I did a good service.
- It was an accident.
- It was not my fault—just an experiment that went bad.
- It was the user's fault because they didn't keep their security up to date.
- If the code didn't alter or delete any of their files, then what's the problem?
- ❖ Computer fraud includes the following:
    - Unauthorized theft, use, access, modification, copying, and destruction of software or data.
    - Theft of money by altering computer records.
    - Theft of computer time.
    - Theft or destruction of computer hardware.
    - Use or the conspiracy to use computer resources to commit a felony.

    - Intent to illegally obtain information or tangible property through the use of computers.

- ❖ In using a computer, fraud perpetrators can steal: More of something, in less time, with less effort

They may also leave very little evidence, which can make these crimes more difficult to detect.

Computer systems are particularly vulnerable to computer crimes for several reasons:

- – Company databases can be huge and access privileges can be difficult to create and enforce. Consequently, individuals can steal, destroy, or alter massive amounts of data in very little time.
- – Organizations often want employees, customers, suppliers, and others to have access to their system from inside the organization and without. This access also creates vulnerability.
- – Computer programs only need to be altered once, and they will operate that way until:
    - The system is no longer in use; or
    - Someone notices

Modern systems are accessed by PCs, which are inherently more vulnerable to security risks and difficult to control.

- It is hard to control physical access to each PC.
- PCs are portable, and if they are stolen, the data and access capabilities go with them.
- PCs tend to be located in user departments, where one person may perform multiple functions that should be segregated.
- PC users tend to be more oblivious to security concerns.

Computer systems face a number of unique challenges:

- Reliability (accuracy and completeness)
- Equipment failure
- Environmental dependency (power, water damage, fire)
- Vulnerability to electromagnetic interference and interruption
- Eavesdropping
- Misrouting

Many computer frauds go undetected. An estimated 80-90% of frauds that are uncovered are not reported because of fear of: Adverse publicity, Copycats, Loss of customer confidence.

There are a growing number of competent computer users, and they are aided by easier access to remote computers through the Internet and other data networks.

- Some folks believe “it can’t happen to us.”
- Many networks have a low level of security.
- Instructions on how to perpetrate computer crimes and abuses are readily available on the Internet.
- Law enforcement is unable to keep up with the growing number of frauds.
- The total dollar value of losses is difficult to calculate.

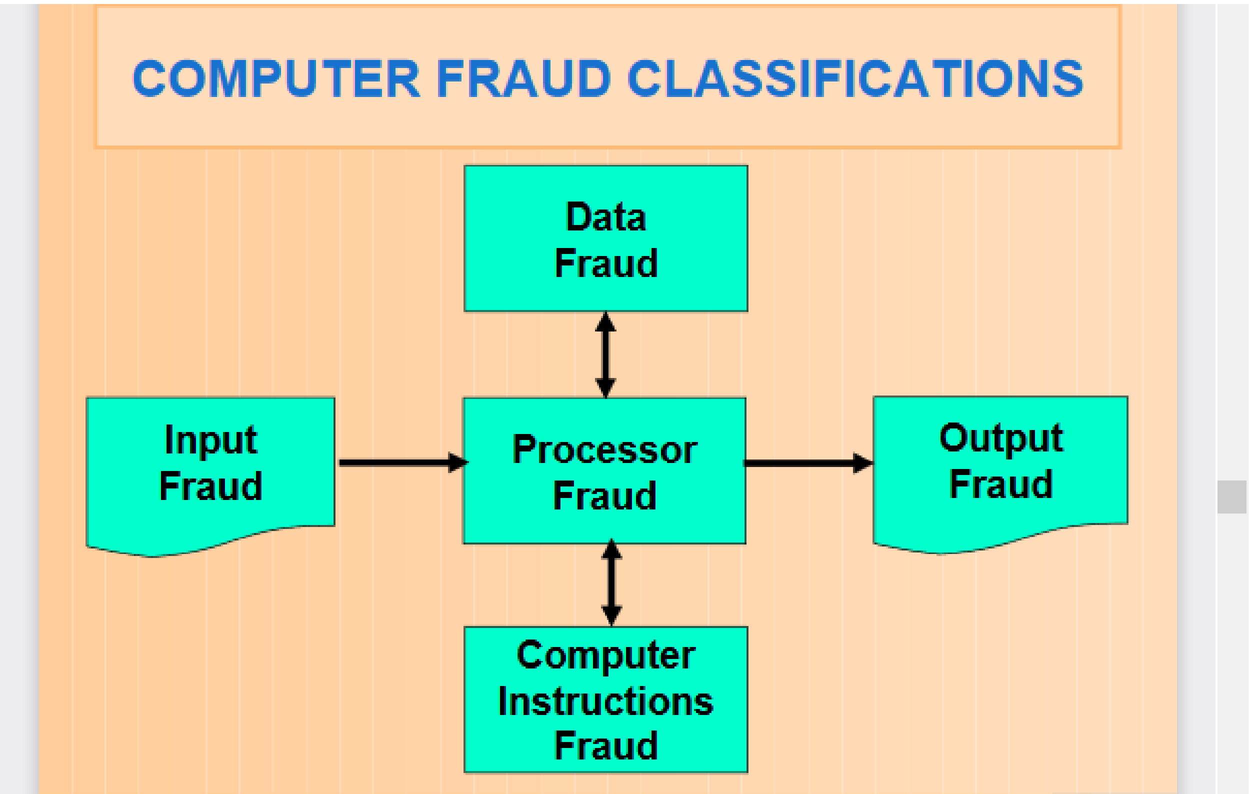
Economic espionage, the theft of information and intellectual property, is growing especially fast. This growth has led to the need for investigative specialists or cyber sleuths.

Computer fraud classification

Frauds can be categorized according to the data processing model:

- Input
- Processor
- Computer instructions
- Stored data
- Output

5.3 Classification of Computer Fraud



COMPUTER FRAUD CLASSIFICATIONS

Data Fraud

Input Fraud

Processor Fraud

Output Fraud

Computer Instructions Fraud

Input Fraud

The simplest and most common way to commit a fraud is to alter computer input. It requires little computer skills, these perpetrator only need to understand how the system operates

Can take a number of forms, including:

a. *Disbursement frauds*. The perpetrator causes a company to: Pay too much for ordered goods; or Pay for goods never ordered.

b. *Inventory frauds*. The perpetrator enters data into the system to show that stolen inventory has been scrapped.

c. *Payroll fraud*. Perpetrators may enter data to: Increase their salaries, Create a fictitious employee, Retain a terminated employee on the records. In the latter two instances, the perpetrator intercepts and cashes the resulting paychecks.

d. *Cash receipt fraud.* The perpetrator hides the theft by falsifying system input. EXAMPLE: Cash of $200 is received. The perpetrator records a cash receipt of $150 and pockets the $50 difference.

e. *Fictitious refund fraud.* The perpetrator files for an undeserved refund, such as a tax refund.

Processor Fraud

- Involves computer fraud committed through unauthorized system use.
- Includes theft of computer time and services.
- Incidents could involve employees:
  - ❖ Surfing the Internet;
  - ❖ Using the company computer to conduct personal business; or
  - ❖ Using the company computer to conduct a competing business.

Computer Instructions Fraud

- Involves tampering with the software that processes company data.–May include:
    - Modifying the software
    - Making illegal copies
    - Using it in an unauthorized manner
- Also might include developing a software program or module to carry out an unauthorized activity.

Computer instruction fraud used to be one of the least common types of frauds because it required specialized knowledge about computer programming beyond the scope of most users. Today these frauds are more frequent--courtesy of web pages that instruct users on how to create viruses and other schemes.

Data Fraud

- Involves:
    - Altering or damaging a company's data files; or
    - Copying, using, or searching the data files without authorization.
- In many cases, disgruntled employees have scrambled, altered, or destroyed data files.
- Theft of data often occurs so that perpetrators can sell the data.
    - Most identity thefts occur when insiders in financial institutions, credit agencies, etc., steal and sell financial information about individuals from their employer's database.

Output Fraud

Involves stealing or misusing system output. Output is usually displayed on a screen or printed on paper. Unless properly safeguarded, screen output can easily be read from a remote location using inexpensive electronic gear. This output is also subject to prying eyes and unauthorized copying. Fraud perpetrators can use computers and peripheral devices to create counterfeit outputs, such as checks.

Specific techniques used to commit computer fraud.

Perpetrators have devised many methods to commit computer fraud and abuse. These include:

1. Data diddling

Changing data before, during, or after it is entered into the system. Can involve adding, deleting, or altering key system data.

2. Data leakage

Unauthorized copying of company data.

3. Denial of service attacks

An attacker overloads and shuts down an Internet Service Provider's email system by sending email bombs at a rate of thousands per second—often from randomly generated email addresses. May also involve shutting down a web server by sending a load of requests for the web pages. Carried out as follows:

- The attacker infects dozens of computers that have broadband Internet access with denial-of-service programs. These infected computers are the zombies. The attacker then activates the denial-of-service programs, and the zombies send pings (emails or requests for data) to the target server. The victim responds to each, not realizing they have fictitious return addresses, and waits for responses that don't come. While the victim waits, system performance degrades until the system freezes up or crashes. The attacker terminates the program after an hour or two to limit the victim's ability to trace the source. A denial-of-service can cause severe economic damage to its victim or even drive them out of business.

4. Eavesdropping

Perpetrators surreptitiously observe private communications or transmission of data. Equipment to commit these "electronic wiretaps" is readily available at electronics stores. A threatening message is sent to a victim to induce the victim to do something that would make it possible to be defrauded. Several banks in the Midwest were contacted by an overseas perpetrator who indicated that:

- He had broken into their computer system and obtained personal and banking information about all of the bank's customers.
- He would notify the bank's customers of this breach if he was not paid a specified sum of money.

5. Email threats

Involves sending an email message that appears to have come from someone other than the actual sender.

6. Email spoofers may:–

- Claim to be system administrators and ask users to change their passwords to specific values.
- Pretend to be management and request a copy of some sensitive information.

7. **Hacking**

Unauthorized access to and use of computer systems—usually by means of a personal computer and a telecommunications network. Most hackers break into systems using known flaws in operating systems, applications programs, or access controls. Some are not very malevolent and mainly motivated by curiosity and a desire to overcome a challenge. Others have malicious intent and can do significant damage.

8. **Phreaking**

Hacking that attacks phone systems and uses phone lines to transmit viruses and to access, steal, and destroy data. They also steal telephone services and may break into voice mail systems. Some hackers gain access to systems through dial-up modem lines.

9. **Hijacking**

Involves gaining control of someone else's computer to carry out illicit activities without the user's knowledge. The illicit activity is often the perpetuation of spam emails.

10. **Identity theft**

Assuming someone's identity, typically for economic gain, by illegally obtaining and using confidential information such as the person's social security number, bank account number, or credit card number. Identity thieves benefit financially by:

- Taking funds out of the victim's bank account.
- Taking out mortgages or other loans under the victim's identity.
- Taking out credit cards and running up large balances.

If the thief is careful and ensures that bills and notices are sent to an address he controls, the scheme may be prolonged until such time as the victim attempts to buy a home or car and finds out that his credit is destroyed.

Identity thieves can steal corporate or individual identities by:

- Shoulder surfing•
    - Watching people enter telephone calling card numbers or credit card numbers or listening to communications as they provide this information to sales clerks or others.

– Scavenging or dumpster diving

- Searching corporate or personal records by rifling garbage cans, communal trash bins, and city dumps for documents with confidential company information.
- May also look for personal information such as checks, credit card statements, bank statements, tax returns, discarded applications for pre-approved credit cards, or other

- records that contain social security numbers, names, addresses, phone numbers, and other data that allow them to assume an identity.

- Redirecting mail
  - Intercepting mail and having it delivered to a location where others can access it.

Using Internet, email, and other technology in spoofing, phishing, eavesdropping, impersonating, social engineering, and data leakage schemes.

The U.S. Department of Justice suggests the following four ways to minimize the chances of being victimized by identity theft:

- Do not give out corporate or personal information unless there is a good reason to trust the person to whom it is given.
- Check financial information regularly for what should be there, as well as for what should not be there.
- Periodically review your credit report.
- Maintain careful records of banking and financial accounts.

11. Internet Misinformation

Using the Internet to spread false or misleading information about people or companies.

May involve: Planting inflammatory messages in online chat rooms. Websites with misinformation. Pretending to be someone else online and making inflammatory comments that will be attributed to that person. A “pump-and-dump” occurs when an individual spreads misinformation, often through Internet chat rooms, to cause a run-up in the value a stock and then sells off his shares of the stock. A number of pump-and-dump cases have been prosecuted by the SEC.

Another common form of Internet misinformation is the spreading of “urban legends”—often by innocently forwarding emails.

- Urban legends may often include damaging implications about company products, such as a recent email suggesting that certain lipsticks contain lead or that using plastic cookware in the microwave can cause cancer.
- Before forwarding any emails with negative information about individuals, companies, or their products, it’s a good idea to check the veracity of the information first.
- Emails with urban legends often attribute their “facts” to credible sources, such as the federal government, Stanford University researchers, the FBI, etc.
- There are several websites that attempt to verify the truth of emails that are circulated. One such website is www.snopes.com. You can easily locate the email you received on these websites, by searching under a key term in the email, such as “lipstick.”
- You are likely to find that most emails you were getting ready to forward are either false or only partially true.

12. Internet terrorism

Hackers use the Internet to disrupt electronic commerce and destroy company and individual communications. Viruses and worms are two main forms of Internet terrorism.

13. Logic time bombs

A program that lies idle until triggered by some circumstance or a particular time. Once triggered, it sabotages the system, destroying programs, data, or both. Usually written by disgruntled programmers. EXAMPLE: A programmer places a logic bomb in a payroll application that will destroy all the payroll records if the programmer is terminated.

14. Masquerading or impersonation

The perpetrator gains access to the system by pretending to be an authorized user. The perpetrator must know the legitimate user's ID and password. Once in the system, he enjoys the same privileges as the legitimate user.

15. Packet sniffers

Programs that capture data from information packets as they travel over the Internet or company networks. Confidential information and access information can be gleaned from the captured data—some of which is later sold.

16. Password cracking

An intruder penetrates a system's defenses, steals the file of valid passwords, decrypts them, and then uses them to gain access to almost any system resources. Sending out a spoofed email that appears to come from a legitimate company, such as a financial institution. EBay, PayPal, and banks are commonly spoofed. The recipient is advised that information or a security check is needed on his account, and advised to click on a link to the company's website to provide the information. The link connects the individual to a website that is an imitation of the spoofed company's actual website. These counterfeit websites appear very authentic, as do the emails.

17. Phishing

One newly graduated college student recently took a job in California and deposited his first paycheck of approximately $5,000 in the bank. That same night, he received an email from the bank, inviting him to click on the link in the email to set up online banking for his new bank account. He followed directions and provided the requested information to set up online banking. Two hours later, he was nervous and called the bank—only to find out that his bank account had been cleaned out and closed. As a rule of thumb, it is a good idea not to click on any link provided in an email and to go directly to the website instead. PayPal, whose email address is commonly spoofed for phishing scams, offers the following advice:

- If PayPal ever sends you an email, they will include your first and last name in the salutation of the email.
- If you need to enter PayPal's website, type "https:" in the URL instead of "http:" in order to enter on the company's secured server.
- If you receive a suspicious email, get out of your browser and go back in before proceeding directly to a company website.

In 2004, a phishing-related scam took place in South America with respect to three large South American banks. Once an individual opened the related email, a script was downloaded on their computer. The script would alter the individual's web browser so that if the user entered the URL of one of these three banks, the browser would redirect them to a counterfeit website for that bank. The oblivious user would provide ID and password information, and was instantly set up for a high-tech robbery of his bank account. Consumer Reports suggests that if you have any questions about the legitimacy of a website, you should try entering the wrong password. A phishing website will typically accept an incorrect password—which cues you that it is a phishing scam.

18. **Piggybacking**

Tapping into a telecommunications line and latching onto a legitimate user before that user logs into a system. The legitimate user unknowingly carries the perpetrator into the system.

19. Social engineering

Perpetrators trick employees into giving them information they need to get into the system. A perpetrator might call an employee and indicate he is the systems administrator and needs to get the employee's password.

20. Software piracy

Copying software without the publisher’s permission. In the U.S., it’s estimated that 26% of software in use is pirated. Fines for individuals and corporations are stiff, and individuals convicted of software piracy can serve jail terms of up to 5 years.

21. **Spamming**

Emailing an unsolicited message to multitudes of people, often in an attempt to sell a product. Many times the product offers are fraudulent. Spammers use creative means to find valid email addresses. Scanning the Internet for addresses posted online. Hacking into company databases and stealing mailing lists.–Staging dictionary (aka direct harvesting) attacks. These attacks use special software to guess addresses at a particular company and send blank emails. Messages not returned are usually valid. These attacks are very burdensome to corporate email systems.

22. **Spyware**

Software that monitors computing habits, such as web-surfing habits, and sends the data it gathers to someone else, typically without the user’s permission.–One type, called adware (for advertising-supported software) does two things: Causes banner ads to pop up on your monitor as you surf the net. Collects information about your Web-surfing and spending habits and forwards it to a company gathering the data—often an advertising or large media organization. Usually comes bundled with freeware and shareware downloaded from the Internet. May be disclosed in the licensing agreement, but users are unlikely to read it. Reputable adware companies claim they don’t collect sensitive or identifying data.

- But there is no way for users to control or limit the activity.
- It is not illegal, but many find it objectionable.

Software has been developed to detect and eliminate spyware, but it may also impair the downloaded software.

- Some is intentionally difficult to uninstall.

23. Keystroke loggers

A keystroke logger records a user’s keystrokes and emails them to or saves them for the party that planted the logger. These are sometimes used by:

- Parents to monitor their children’s computer usage.
- Businesses to monitor employee activity.
- Fraudsters to capture passwords, credit card numbers, etc.
- A keystroke logger can be a hardware device attached to a computer or can be downloaded on an individual’s computer in the same way that any Trojan horse might be downloaded.

Spyware and keystroke loggers are very problematic for companies with employees who telecommute or contact the company’s computer from remote locations. Spyware on those computers makes the company’s systems vulnerable. Individuals are also exposed when they use wireless networks, such as those that may be available in coffee shops.

24. **Superzapping**

Unauthorized use of special system programs to bypass regular system controls and perform illegal acts. The name is derived from an IBM software utility called Superzap that was used to restored crashed systems.

25. **Trap doors**

Also called back doors. Programmers create trap doors to modify programs. The trap door is a way into the system that bypasses normal controls. The trap door should be removed before the program is implemented. If it is not, the programmer or others may later gain unauthorized access to the system.

26. Trojan horse

A set of unauthorized computer instructions planted in an authorized and otherwise properly functioning program. Allows the creator to control the victim's computer remotely. The code does not try to replicate itself but performs an illegal act at some specific time or when some condition arises. Programs that launch denial of service attacks are often Trojan horses.

27. War dialing

Hackers search for an idle modem by programming their computers to dial thousands of phone lines. Hackers enter through the idle modem and gain access to the connected network.

28. War driving

Driving around in cars looking for unprotected home or corporate wireless networks. If the hackers mark the sidewalk of the susceptible wireless network, the practice is referred to as *warchalking.*

29. Virus

Many viruses have two phases:

i. First, when some predefined event occurs, the virus replicates itself and spreads to other systems or files.

ii. Another event triggers the attack phase in which the virus carries out its mission. A virus may lay dormant or propagate itself without causing damage for an extended period.

Damage may take many forms:

- Send email with the victim's name as the alleged source.
- Destroy or alter data or programs.
- Take control of the computer.
- Destroy or alter file allocation tables.
- Delete or rename files or directories.
- Reformat the hard drive.
- Change file content.
- Prevent users from booting.
- Intercept and change transmissions.
- Print disruptive images or messages on the screen.
- Change screen appearance.

As viruses spread, they take up much space, clog communications, and hinder system performance.

5.3.1 Virus symptoms:

Computer will not start or execute, Performs unexpected read or write operations, Unable to save files, Long time to load programs, Abnormally large file sizes, Slow systems operation, Unusual screen activity and Error messages

Viruses are contagious and easily spread from one system to another. They are usually spread by: Opening an infected email attachment or file (most common); or, Running an infected program.

Some viruses can mutate, which makes them more difficult to detect and destroy. The emails often appear to come from sources like Microsoft and seem very convincing.

5.4 Virus protections include:

– Install reliable virus software that scans for, identifies, and destroys viruses.

- Keep the antivus program up to date.
- Scan incoming email at the server level, rather than when it hits the desktops.
- Certify all software as virus-free before loading it.
    - Software from unknown sources may be virus bait, especially if it seems too good to be true.
- Deal with trusted software retailers.
- Use electronic techniques to make tampering evident.
- Check new software on an isolated machine.
- Have two backups of all files.
- Do not put diskettes or CDs in strange machines, or let others put unscanned disks in your machine.

Viruses attack computers, but any device that is part of the communications network is vulnerable, including:

- Cell phones, Smart phones and PDAs

A worm is similar to a virus except for:

A worm is a stand-alone program, while a virus is only a segment of code hidden in a host program or executable file. A worm will replicate itself automatically, while a virus requires a human to do something like open a file. Worms often reproduce by mailing themselves to the recipient's mailing list. They are not confined to PCs and have infected cell phones in Japan. A worm typically has a short but very destructive life. It takes little technical knowledge to create worms or viruses; several websites provide instructions. Most exploit known software vulnerabilities that can be corrected with a software patch, making it important to install all patches as soon as they are available.

You receive an email from a friend, apologizing profusely that he/she has previously sent you an email that was infected with a virus. The friend's email gives you instructions to look for and remove the offending virus. You delete the file from your hard drive. The only problem is that the file you just deleted was part of your operating system. Your friend was well-intended and has done the same thing to his/her computer.

5.5 REMEDY:

Before even considering following instructions of this sort, check the list of hoaxes that are available on any virus protection website, such as:–www.norton.com and www.mcafee.com

Way that company can deter and detect computer fraud

Organizations must take every precaution to protect their information systems. Certain measures can significantly decrease the potential for fraud and any resulting losses. These measures include:

a. Make fraud less likely to occur
b. Increase the difficulty of committing fraud
c. Improve detection methods
d. Reduce fraud losses

1. ***Make fraud less likely to occur***

- Create a culture that stresses integrity and commitment to ethical values and competence.
- Adopt an organizational structure, management philosophy, operating style, and appetite for risk that minimizes the likelihood of fraud.
- Require oversight from an active, involved, and independent audit committee.
- Assign authority and responsibility for business objectives to specific departments and individuals, encourage initiative in solving problems, and hold them accountable for achieving those objectives.
- Identify the events that lead to increased fraud risk, and take steps to prevent, avoid, share, or accept that risk.

- Develop a comprehensive set of security policies to guide the design and implementation of specific control procedures, and communicate them effectively to company employees.
- Implement human resource policies for hiring, compensating, evaluating, counseling, promoting, and discharging employees that send messages about the required level of ethical behavior and integrity.
- Effectively supervise employees, including monitoring their performance and correcting their errors.
- Train employees in integrity and ethical considerations, as well as security and fraud prevention measures.
- Require annual employee vacations, periodically rotate duties of key employees, and require signed confidentiality agreements.
- Implement formal and rigorous project development and acquisition controls, as well as change management controls.
- Increase the penalty for committing fraud by prosecuting fraud perpetrators more vigorously.

2. Increase the difficulty of committing fraud

- Develop a strong system of internal controls–Segregate the accounting functions of:
  - Authorization
  - Recording
  - Custody
- Implement a program segregation of duties between systems functions
- Restrict physical and remote access to system resources to authorized personnel.
- Require transactions and activities to be authorized by appropriate supervisory personnel. Have the system authenticate the person and their right to perform the transaction before allowing the transaction to take place.–Use properly designed documents and records to capture and process transactions.
- Safeguard all assets, records, and data.
- Require independent checks on performance, such as reconciliation of two independent sets of records, where possible and appropriate.
- Implement computer-based controls over data input, computer processing, data storage, data transmission, and information output.
- Encrypt stored and transmitted data and programs to protect them from unauthorized access and use.
- Fix known software vulnerabilities by installing the latest updates to operating systems, security, and applications programs.

3. Improve detection methods.

- Create an audit trail so individual transactions can be traced through the system to the financial statements and vice versa.
- Conduct periodic external and internal audits, as well as special network security audits.
- Install fraud detection software.
- Implement a fraud hotline.
- Employ a computer security officer, as well as computer consultants and forensic specialists as needed.
- Monitor system activities, including computer and network security efforts, usage and error logs, and all malicious actions.

- Use intrusion detection systems to help automate the monitoring process.

4. ***Reduce Fraud Losses***

- Maintain adequate insurance.
- Develop comprehensive fraud contingency, disaster recovery, and business continuity plans.
- Store backup copies of program and data files in a secure, off-site location.
- Use software to monitor system activity and recover from fraud.

5.5 Summary

In this chapter, you've learned what fraud is, who commits fraud, and how it's perpetrated. You've learned about the many variations of computer fraud, and you've learned about techniques to reduce an organization's vulnerability to these types of fraud.

Reading materials/list

1. Romney, M.B. & Steinhart, P.J (2005 & 2006). Accounting information systems, 10th edition upper saddle river.
2. Hall & singleton (2005). Information systems auditing and assurance 2nd edition
3. McMahon D (2009). Accounting information systems, 1st edition, Pearson. Publishers UK.
4. Boczko, T (2007). Corporate accounting information systems 1st edition Prentice Hall UK.