Chapter 8:
Security and Control,
System Development Life Cycle

Ethics and Social Issues

What are Computer Ethics?

- Moral guidelines that govern use of computers and information systems
  - Unauthorized use of computer systems
  - Information privacy
  - Intellectual property rights
  - Software theft (piracy)
  - Information accuracy
  - Codes of conduct

What do you think about ethical issues?

	ETHICAL	UNETHICAL
1. A company requires employees to wear badges that track their whereabouts while at work.	☐	☐
2. A supervisor reads an employee's e-mail.	☐	☐
3. An employee uses his computer at work to send e-mail messages to a friend.	☐	☐
4. An employee sends an e-mail message to several co-workers and blind copies his supervisor.	☐	☐
5. An employee forwards an e-mail message to a third party without permission from the sender of the message.	☐	☐
6. An employee uses her computer at work to complete a homework assignment for school.	☐	☐
7. The vice president of your Student Government Association (SGA) downloads a photograph from the Web and uses it in a flier recruiting SGA members.	☐	☐
8. A student copies text from the Web and uses it in a research paper for his English Composition class.	☐	☐
9. An employee sends political campaign material to individuals on her employer's mailing list.	☐	☐
10. As an employee in the registration office, you have access to student grades. You look up grades for your friends so they do not have to wait for delivery of grade reports from the postal service.	☐	☐

Why is Information Accuracy Important?

- Inaccurate input can result in erroneous information and incorrect decisions based on that information
- Evaluate Web page's value before relying on its content

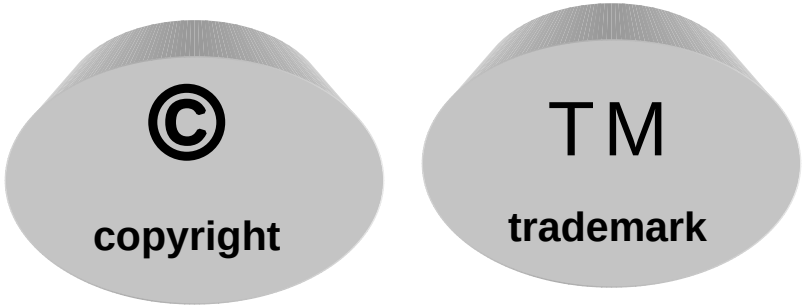
Evaluation Criteria	Reliable Web Pages
Audience	The Web page should be written at an appropriate level.
Authority	The Web page should list the author and the appropriate credentials.
Affiliation	A reputable institution should support the Web site without bias in the information.
Content	The Web page should be well organized and the links should work.
Currency	The information on the Web page should be current.
Design	The Web site should load quickly, and be pleasing visually and easy to navigate.
Objectivity	The Web page should contain little advertising and be free of bias.

What are the Ethics of Using Computers to Alter Output?

- Alteration could lead to deliberately misleading photographs

Intellectual Property Rights

- Intellectual property (IP) refers to work created by inventors, authors, and artists
- Intellectual property rights are rights to which creators are entitled for their inventions, writings, and works of art



IT Code of Conduct

- Written guideline that helps determine whether specific computer action is ethical or unethical

1. Computers may not be used to harm other people.
2. Employees may not interfere with other's computer work.
3. Employees may not meddle in other's computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use other's computer resources without authorization.
8. Employees may not use other's output.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

Security and Control, System Development Life Cycle

Security and Control

Security and Controls

- Data, software and hardware are valuable resources and must be kept secure from being wrongly changed or being destroyed accidentally or deliberately.
- Data must also be secured against wrongful disclosure.
- A hardware fault or a telecommunications fault, can suffer financial loss.
- Confidential data which is being word processed might be vulnerable to unauthorized access.
- The Data Protection Act 1994 incorporates a principle that computerized personal data be kept secure against wrongful disclosure.
- If computerized data is not protected properly, there will also be scope for computer fraud.

Problems Associated with Computers

- Data processing by computer created extra problems for control because of its special characteristics:
  - Inaccuracy of Programs and Data
  - Lose Data on File
  - Unauthorized Access
  - No Logging and Tracing
  - Dishonest Programmers
  - Accidental Error Cause Problems

Problems Associated with Computers - Inaccuracy of Programs and Data

- Large volumes of data are concentrated into files that are physically very small.
- Large quantities of data are processed without human intervention, and so without humans knowing what is going on.
- This places great reliance on the accuracy of programs and of data on file.

Problems Associated with Computers - Lose Data on File

- Equipment can malfunction, data files can become corrupt and store meaningless data, data can get lost when files are copied, and data files are susceptible to loss through theft, flood or fire.

Problems Associated with Computers - Unauthorized Access

- Unauthorized people can gain access to data on files, and read confidential data or tamper with the data.
- This is a particular problem with on-line systems because access to a computer program and master file can be from any remote terminal.
- It is even possible for Hacker to use their computers to gain access to files and programs of other systems.

Problems Associated with Computers - No Logging and Tracing

- Information on a computer file can be changed without leaving any physical trace of the change.
- It does not help matters that computers lack judgment and errors in data processing by computer can go undetected when this would not be the case with manual data processing.

Problems Associated with Computers - Dishonest Programmers

- Programmers are experts, and with careful planning, dishonest programmers can tamper with programs to their own benefit.
- A case has been recorded, for example, of a programmer who arranged for all fractions of a penny in salaries to be paid into a bank account which the programmer opened and from which he took the money.
- Several thousand payments mounted up over time into substantial sums of money.

Problems Associated with Computers - Accidental Error Cause Problems

- What is to stop a computer operator from using a disk containing master file data to take output from a different program?
- If this were done, the data on the master file could be wiped out.
- This is such an important source of potential error that controls to prevent this from happening should be built into nay computer system.

Types of Security Risks

- Types of security risks that can threaten your computers:
  - Manipulation and Sabotage
  - Natural Disasters
  - Procedural Failures

Types of Security Risks - Manipulation and Sabotage

- Data and information can be stolen, destroyed, modified by an authorized person
  - Examples: Hacking, Fraud
- The impact of this threat will affect the loss of confidentiality, availability and integrity of data
- When the information is stolen, it causes loss of confidentiality.
- When it is destroyed, it causes loss of availability
- When it is modified, it causes the loss of integrity.

Types of Security Risks - Natural Disasters

- Natural disasters are natural events that occur outside the control of mankind.
  - Examples: typhoon, fore, earthquake, flood.
- These are threats, which can bring about loss of availability as they destroy the hardware and software hosting the data

Types of Security Risks - Procedural Failures

- These threats are caused by failure or non-existence of adequate procedures.
- Uncontrolled access to the computer room and IT equipment would be examples of procedural failures.
- This threat can cause the lost of availability as staff might accidentally destroy or misplace diskettes.
- It can also cause the loss of confidentiality as staff would be able to leak information or sell information to other companies.
- It can also cause the loss of integrity if the staff modifies data with malicious or mischievous intent.

The Need for Security and Controls

- Computer systems controls must be maintained regardless of the size of application or method of processing (batch or real time).
- If certain controls are difficult to establish in a microcomputer system (for example, division of responsibilities), more emphasis must be placed on other controls.

The Risks to Data

- The dangers associated with information storage magnetic medium include the following:
  - Physical Security
  - Environmental Security
  - Loss of Confidentiality
  - Processing the Wrong File
  - Hardware or Program Corruption

The Risks to Data – Physical Security

- Tapes or disks can be stolen, mislaid or damaged or destroyed by fire, flood or vandalism.

The Risks to Data – Environmental Security

- Tapes and disks are susceptible to magnetic fields, dust and extremes of temperature and humidity.
- Although in modern PCs the problems of environmental control have been reduced, they are still quite important.

The Risks to Data – Loss of Confidentiality

- Information stored in magnetic fields may be accessed by unauthorized persons.
- This is a particular problem in larger systems with remote terminals, or in time sharing or computer bureau applications.

The Risks to Data – Processing the Wrong File

- Since data is in magnetic form, and not visible, the wrong file could be read, or a file could be overwritten when its data is still needed.

The Risks to Data – Hardware or Program Corruption

- Hardware or software faults may damage or destroy the data on files.

Controls

- Controls which can be implemented to counter the risks fall into two categories.
  - **General Controls** ensure that the computer environment is secure. They fall into two groups.
    - **Administrative Controls** are designed to support the smooth continuing operation of systems.
    - **System Development Controls** are designed to ensure that any new system does not present new risks to the environment.
  - **Application Controls** are built into operations, and ensure that processed data is accurate and complete.

Administrative Controls

- Some controls can be applied at relatively small cost, simply by introducing sensible administrative and organizational measure.
- Administrative controls are controls over data and data security that are achieved by administrative measures.
- They should be applied in the data processing department, or computer centre, where an organization is large enough to have one, and in other offices.
- With PC systems, administrative controls will include controls over handling the computer hardware, software and files.

Administrative Controls

- Administrative controls should include:
  - Controls over Personnel
  - The Segregation of Duties
  - Physical Security
  - Access Controls
  - Protection Against Hacking and Viruses
  - Good Office Practice
  - Back-up and Standby Facilities

Controls over Personnel

- Controls related to personnel, which were developed before the advent of computers:
  - Job rotation
  - Enforced vacations
  - Access to information granted not on the basis of rank in the management hierarchy or precedent, but on a need-to-know basis
- Some employees, such as the systems analyst and the computer security officer, are always in a position of trust.
- A well-designed security system puts a few people as possible in this powerful position.

The Segregation of Duties

- Work should be divided between systems analysts, programmers and operating staff, and operations jobs themselves should be divided between data control, data preparation and computer room operations.
- The functions of an organization structure are:
  - To assign responsibility for certain tasks to specific jobs and individuals.
  - To prevent fraud.
- Duties may be segregated by ensuring that no member of staff works more than of:
  - Data capture and entry
  - Computer operations
  - Systems analysis and programming

Physical Security

- Physical security comprises two sorts of controls:
  - Protection against disasters such as fire and flood
  - Protection against intruders gaining physical access to the system

Physical Security – Protection Against Disasters

- The physical environment has a major effect on information system security and so planning it properly is an important part of an adequate security plan.
- Protection against disasters includes:
  - Site preparation
  - Site surveys for potential structural damage (all types of physical disaster)
  - Detection of fire and smoke
  - Have extinguishers or sprinklers
  - Off-site recovery systems
  - Flood warning system
  - Flood defense systems
  - Conduct drills / simulated disasters
  - Training for Staff in Observing Fire Safety Procedures

Physical Security – Protection Against Disasters (Cont')

- Site Preparation
  - Involves the preparation of the site against fire or flood
- Extinguisher system
  - Involves the use of a system that can extinguish the fire and yet preserve data. Gas extinguishing systems are commonly used.
- Detection system
  - Involves the implementation of a good detection system using technologies such as infrared or image recognition so as to detect fires early.
- Fire readiness procedures
  - Involves the preparation of staff to react accordingly in the event of a fire.

Physical Security – Protection Against Intruders

- **Personnel (Security Guards)**
  - Unauthorized persons must be prevented from physical access to the sensitive areas. Therefore, physical control can be enforced by means of Room Partitions or Security Guards.
- **Mechanical Devices**
  - Mechanical Devices could be used to secure access to critical resources.
- **Electronic Identification Devices**
  - Electronic Identification Devices can be used to determine accurately the identity of the person who requires access to the data resources.

Physical Security – Physical Installation Security

- Regularly backups of data and programs must be made so that recovery of the systems can be done easily in the vent of a data compromise.
  - Sensitive rooms should always be locked and are accessible only to authorized personnel.
  - Sensitive files should be kept in safe place or remote site.

Physical Security Measurement

- Physical security measurement to protect IT assets
  - Lock rooms
  - Use fire-proof safes
  - Off-site backups
  - Minimize public knowledge of installation (don't advertise its location)

Access Controls

- Access controls are controls designed to prevent unauthorized access to data files or programs.
- Access controls which can be built into system's software are:
  - Passwords
  - Encryption and Authentication (Data Communications Controls)

Passwords

- Passwords can be applied to data files, program files an parts of a program.
- The computer does not allow a user access to the relevant facilities until he has typed in the appropriate password.
  - One password may be required to read a file and another to write new data.
  - The terminal user can be restricted to the use of certain files and programs.

Limitation of Passwords

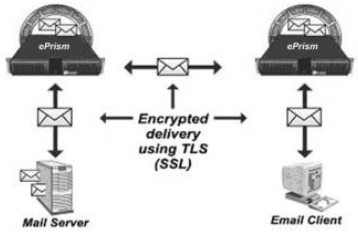
- Passwords ought to be effective in keeping out unauthorized users, but they are by no means foolproof.
- Experience has shown that unauthorized access can be obtained.
  - By experimenting with possible passwords, an unauthorized person can gain access to a program or file by guessing the correct password.
  - Someone who is authorized to access a data or program file may tell an unauthorized person what the password is, perhaps through carelessness.

Encryption and Authentication

- When data is transmitted over a communication link or within a network, there are three security dangers:
  - A hardware fault
  - Unauthorized access by an eavesdropper
  - Direct intervention by someone who sends false messages down a line, claiming to be someone else, so that the recipient of the message will think that it has come from an authorized source.

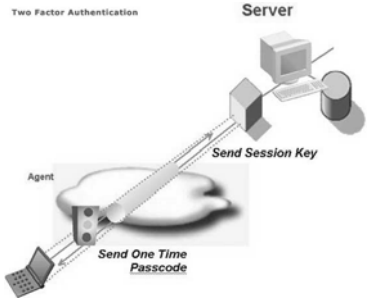
What is Encryption?

- Encryption is the only secure way to prevent eavesdropping.
- Encryption involves scrambling the data at one end of the line, transmitting the scrambled data and unscrambling it at the receiver's end of the line.



What is Authentication ?

- Authentication is a technique to make sure that a message has come form an authorized sender.
- Authentication involves adding an extra field to a record, with the contents of this field derived from the remainder of the record by applying a formula that has previously been agreed between senders and the recipients of data.



Protection against Hacking and Viruses

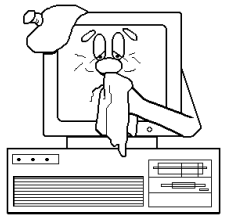
- As it becomes common for computers to communicate over long distances, the risk of corruption or theft of data or even whole programs becomes much greater.
- Two interconnected security issues are **Hacking** and **Viruses**.

Hacking

- A **Hacker** is a person who attempts to invade the privacy of a computer system.
- Hackers are normally skilled programmers and have been known to find out passwords with ease.
- The fact that billions of bits of information can be transmitted in bulk over the public telephone network has made it hard to trace individual hackers, who can therefore make repeated attempts to invade systems.
- Hackers have in the past mainly been concerned to copy information, but a recent trend has been their desire to corrupt it.

Viruses

- A computer virus is a piece of software which infects programs and data and which replicates itself.
- Viruses can spread via data disks, but have been known to copy themselves over whole networks.
- The most serious type of virus is one which infects an operating system as this governs the whole running of a computer system.
- There are a number of types of virus.
  - A Trojan
  - A time bomb
  - A trap door



Viruses – Trojan

- A Trojan is a program is a piece of code triggered by certain events.
- A program will behave normally until a certain event occurs, for example disk utilization reaches a certain percentage.
- A logic bomb, by responding to such conditions, maximizes damage.
  - For example, it will be triggered when a disk is nearly full, or when a large number of users are using the system.

Viruses – Time Bomb

- A time bomb is similar to a logic bomb except that it is triggered at a certain date.
- Companies have experienced virus attacks on April Fool's Day and on Friday 13th .
- These were released by time bombs.

Viruses – Trap Door

- A trap door is not itself a virus, but it is an undocumented entry point into a computer system.
- It is not to be found in design specifications but may be put in by software developers to enable them to bypass access controls while working on a new piece of software.
- Because it is not documented, it may be forgotten and used at a later date to insert a virus.

Protection Against Viruses

- How can organizations protect themselves against viruses?
  - Vaccine programs exist which can deal with some viruses, but if the virus lives in the bootstrap program, the virus can work before the vaccine is loaded.
  - Organizations must guard against the introduction of unauthorized software to their systems.
  - Organizations should as a matter of routine ensure that any risk received from outside with data on it is virus-free before the disk is used.
  - Any flaws in a widely used program should be rectified as soon as they come to light
  - There should be a clear demarcation between the storage of data files and program files on disk.
  - Organizations need to establish procedures and reviews to minimize the chances of infection. Virus protection controls should become part of the internal control system of an organization.

Good Office Practice

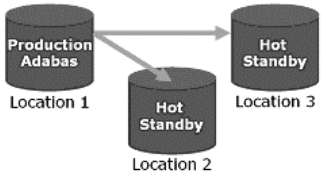
- There are several points of good practice which can together make a major contribution to the integrity of a system.
  - Data is often shared between users. There should be a designated data owner for each file, responsible for:
    - Keeping data accurate and up to date
    - Deciding who should have access to the data
    - Developing security procedures in conjunction with the data security manager
  - If a computer printout is likely to include confidential data, it should be shredded before being thrown away.
  - Disks should not be left lying around an office.
  - The computer's environment (humidity, temperature and dust) should be properly controlled.
  - Files should be backed up regularly.

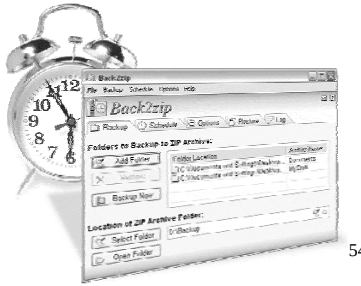
Maintenance and Support

- All computers are covered by some kind of warranty from the manufacturer when they are bought new. What should the computer user do after the warranty period has expired?
  - Ask a third party computer repair company to come in and do the repair work. The drawbacks to this are that:
    - Repair companies give priority treatment to contract customers.
    - One-off repair charges will be very high.
  - The user can arrange a maintenance contract with the manufacturer or a third party repair company.
  - A third option is breakdown insurance, which provides cover for breakdowns and certain consequential losses.

Back-up and Standby Facilities

- A major aspect of system security is to ensure provision of the required services continuously without deterioration in performance.
- For many applications this will require that some duplication in the system be tolerated or even discouraged.
- Administrative controls should be introduced:
  - To enable file data to be recreated when a file is lost or corrupted;
  - To provide stand-by hardware facilities whenever a hardware item breaks down.





Recreating File Data when a File is Lost or Corrupted

- One of the worst things that could happen in data processing by computer is the loss of all the data on a master file or the loss of a program.
- Files might be physically lost, physically damaged and become unreadable.
- Controls are therefore needed to enable a data or program file to be created if the original is lost or corrupted.

Business Continuity Planning

- A disaster is any security event which can cause a significant disruption to the IT capabilities for long enough to affect the operations of an organization.
- Organizations must prepare for disasters so that they are able to recover form one should it happen.
- A **Disaster Recovery Plan** (DRP) is also known as a **Contingency Plan** or a **Business Continuity Plan** (BCP).

Resumption after a Crisis

- The key to successful recovery is adequate preparation.
- Seldom does a crisis destroy irreplaceable equipment; most computing equipment systems – personal computers to mainframes – are standard, "off the shelf" systems that can easily be replaced.
- Data and locally developed programs are more vulnerable, since these cannot be quickly substituted from another source.

Backup

- A **Backup** is a copy of all or part of a file to assist in re-establishing a lost file.
- A **Complete Backup** is copying everything on the system (including system files, user files, scratch files, and directories) and done at regular times, so that the system can be regenerated after a crisis.
- In critical transaction systems this problem is solved by keeping a complete record of changes since the last backup.
- If a system handles bank teller operations, the individual tellers duplicate their processing on paper records; if the system fails, people can start with the backup version and reapply all changes from the collected paper copies.

Off-site Backup

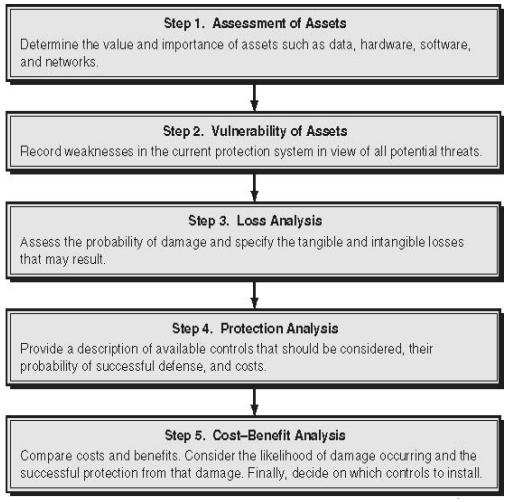
- A backup copy is useless if it is destroyed in the crisis.
- Major computing installations rent warehouse space some distance from the computing system, in some cases 15 or 20 miles away.
- As a backup is completed, it is transported to the backup site.
- Keeping a backup version separate from the system reduces the risk of its loss.
- Similarly, the paper trail is also stored somewhere other than at the main computing facility.

Auditing

- Implementing controls in an organization can be very complicated and difficult to enforce. Are controls installed as intended? Are they effective? Did any breach of security occur? These and other questions need to be answered by independent and unbiased observers. Such observers perform an auditing task.
- There are two types of audits.
  - The **Operational Audit** determines whether the IT department is working properly.
  - The **Compliance Audit** determines whether controls have been implemented properly and are adequate.

Risk Management

- It is usually not economical to prepare protection against every possible threat.
- An IT security program must provide a process for assessing threats and deciding which ones to prepare for and which ones to ignore.



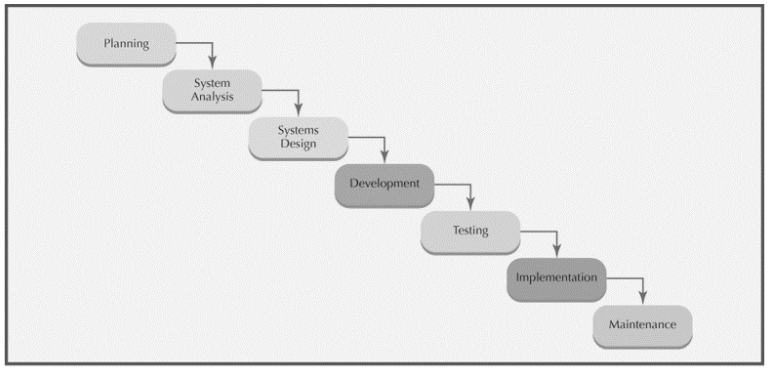
Security and Control, System Development Life Cycle

System Development Life Cycle

What is System Development Life Cycle ?

- The **System Development Life Cycle** (SDLC) is the set of activities that analysts, designers and users carry out to develop an implement an information system.

Figure 11.1 Systems Development Life Cycle (SDLC)



System Development Life Cycle

- The **System Development Life Cycle** (SDLC) method is classically thought of as the set of activities that analysts, designers and users carry out to develop and implement an information system.
- In most business situations, the activities are all closely related, usually inseparable, and even the order of the steps in these activities may be difficult to determine.
- Different parts of a project can be in various phases at the same time, with some components undergoing analysis while others are at advanced design stages.

System Development Life Cycle

- The systems development life cycle method consists of the following phases:
  - Preliminary Investigation (include Feasibility Study)
  - Determination of System Requirements
  - Design of System
  - Development of Software (include Programming)
  - Systems Testing
  - Implementation
  - Post-implementation

Preliminary Investigation

- A request to receive assistance from information systems can be made for many reasons, but in each case someone (a manager, an employee, or a systems specialist) initiates the request.
- The major task in this phase is the **Feasibility Study**.
- The key issue is to determine the likelihood of success in the project such as examining which technology to be used.
- The **Costs and Benefits** of the project would also be evaluated to ensure that the project has positive returns.

Determination of Systems Requirements

- The analysts would study the existing system and examine the problems.
- As the details are gathered, the analysts identify features the new system should have, including both the information and the system should produce and operational features such as processing controls, response times, and input and output methods.
- The user plays a major role in defining their requirements.

Design of System

- The design of an information system produces the details that state how a system will meet the requirements identified during systems analysis.
- There are various aspects to systems design.
  - Design the Input
  - Design the Processing
  - Design the Output
  - Design the Storage

Design of System – Design the Input

- The systems design also describes how data is to input.
- This includes the design of input screens, etc.

Design of System – Design the Processing

- The systems design also describes how the data will be processed.
- Individual data items and calculation procedures are written in detail.

Design of System – Design the Output

- Systems analysts begin the design process by identifying reports and other output the system will produce.
- Then the specific data on each are pinpointed.
- Designers sketch the form or display as they expect it to appear when the system is complete.
- This may be done on paper or on a computer display, using one of the automated system design tools available.

Design of System – Design the Storage

- Designers define the database and select storage devices, such as magnetic disk, magnetic tape, or even paper files.

Development of Software

- When the system design is approved, the detailed development work begins.
- This involves the actual programming work together with database setup etc. that are all bases on the systems design.

Systems Testing

- During systems testing, the testing is used experimentally to ensure that the software does not fail.
- Special test data are input for processing, and the results examined.
- A limited number of users may be allowed to use the system so analysts can see whether they try to use it in unforeseen ways.
- It is preferable to discover any surprises before the organization implements the system and depends on it.
- In many organizations, testing is performed by persons other than those who wrote the original programs to ensure more complete and unbiased testing and more reliable software.

Implementation

- Many activities take place during the implementation phase.
- Each of these is done to prepare the user or the environment for the operational usage of the system that has been developed.
  - Site Preparation
  - Training

Implementation – Site Preparation

- The worksite must be prepared before the system can be used operationally.
- Workstations must be set up with adequate space for the personal computer, printer, modem, etc.
- Power supply and lights must be installed or enhanced. Then the actual equipment must be installed and tested.

Implementation – Training

- Training must be conducted for the users of the system and this usually takes the form of classroom training.

Post-Implementation

- The activities which take place immediately after cutover are onsite support and the Post-Implementation Review.
  - Onsite Support
  - Post-Implementation Review (PIR)

Post-Implementation – Onsite Support

- Initial teething problems are expected and the IT professionals should provide onsite assistance to users.

Post-Implementation – PIR

- The post-implementation review is an evaluation or both the process and product quality.
- The strengths and weaknesses of the system are discussed with a view to improving it.
- Similarly, the process of its development, the SLDC, is reviewed with the intention of learning from mistakes.

Advantages of Traditional SDLC

- Formal review at the end of each phase allows maximum management control
- This approach creates considerable system documentation
- Formal documentation ensures that systems requirement can be traced back to stated business needs
- It produces many intermediate products that can be reviewed to see whether they meet the user's needs & conform to standards

Disadvantages of Traditional SDLC

- Users get a system that meets the needs as understood by the developers; this may not be what was really needed
- Documentation is expensive and time-consuming to create. It is also difficult to keep current
- User needs are unstated or are misunderstood
- Users cannot easily review intermediate products and evaluate whether a particular product (e.g. DFD) meets their business requirements

Main Participants for SDLC

SDLC Stage	Main Participants
Preliminary Investigation	Management involvement only
Determination of system requirements	Mainly Users
Systems Design	All users
Systems Development	Programmers involved
Systems Testing	All staff
Systems Implementation	All staff
Post-system implementation	Management and Staff