) Information Systems (IS)

finitions : IS is made up of two terms namely

1. Information
2. System

- Information can be defined as a well structured data with a specific meaning

- System can be defined as an arrangement that takes inpu & provides output after completing the process.

- IS is an arrangement that processes data and provides meaningful information.

- IS is a set of interrelated components that
  - collect
  - store
  - process
  - generate
  - disseminate information for effective business functioni

urces of components of IS :

Collection - Inter organization and Intra organization

Storage - Paper & electronic format

Processing is done by calculating, analyzing, logical analysis

transformation is done by processing data obtained and transformin

Dissemination - The information (data after transforming) is

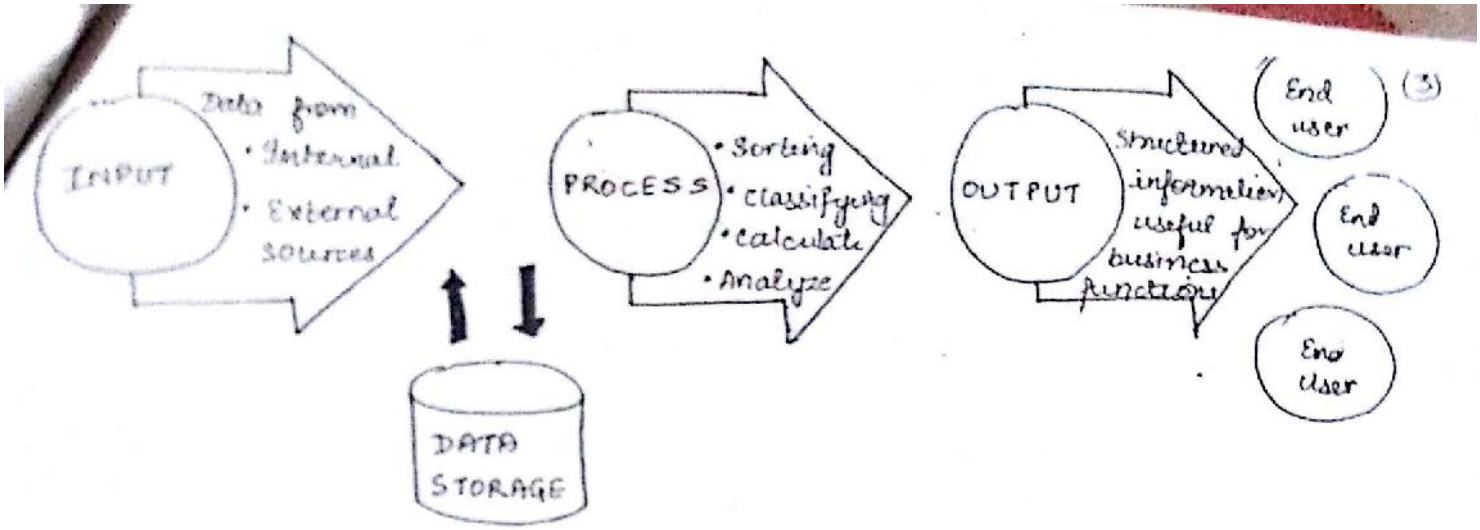


Fig. Displaying the IS Model

Computer literacy and IS Literacy

Basis	Computer Literacy	IS Literacy
Coverage	Knowledge about various components of computer system	Knowledge about accessing, organizing evaluating and using data from various sources.
Scope	It involves computer Science discipline.	It involves the IS application.
Relation with each other	It improves IS effiency.	It helps to utilize computer systems better.

IS Components

1. System Resources – People, Hardware, Software, Data, Network
2. System Activities – Input, Storage, Process, Output, Control & Maintenance

1) IS Resources :

- People — IS specialists : Sys. Anal., Sys. analyst
  - End users
- Hardware — Machine component : Monitor, printer etc.
  - Media Component : pen drives, floppy disc
- Software — Programs : O.S. & Appl.° sys
  - Procedures : data entry & info. distribution
- Data
- Network

Internal sources : prod. descriptions, cust. records etc.

External sources : supplier details, competitor information

- Comm" Component — ex: network access
- Media component — ex: control software

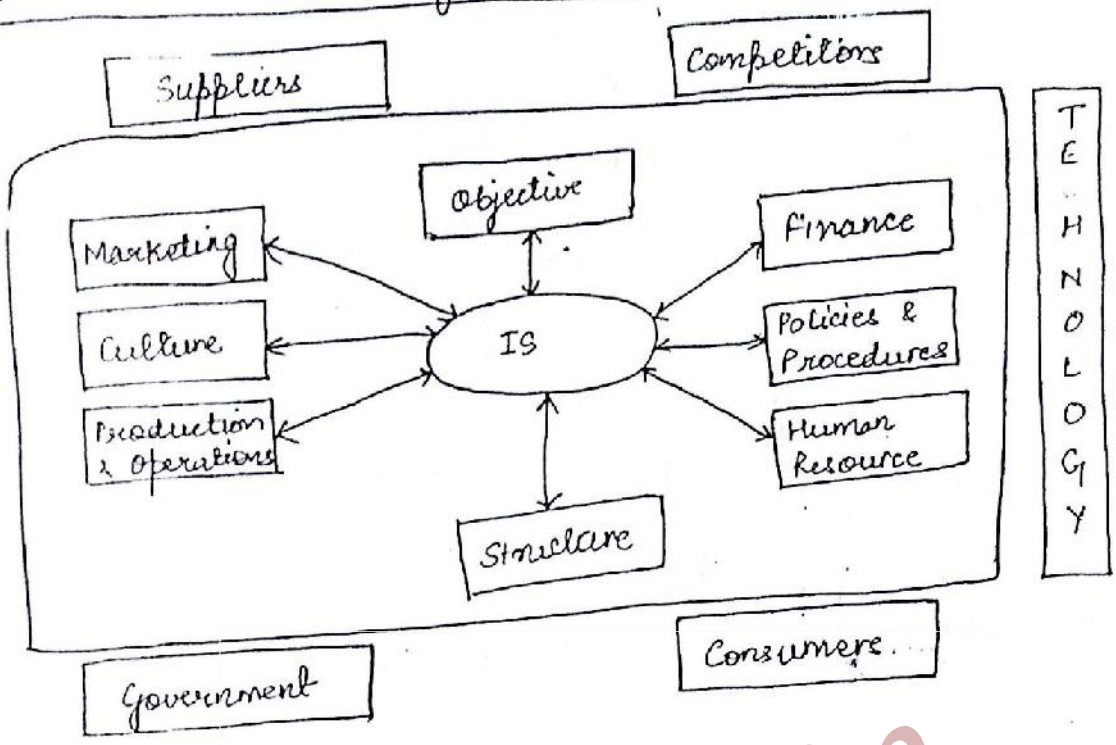
IS Activities :

- Input — Data entry activities like recording & editing.
- Data Storage — Maintaining & organizing records
- Processing Activities like classifying, calculating etc.
- Output — Communicating the processed info. to end users
- Control & system maintenance — Feedback at each activity level to maintain the standard performance.

Trends in IS

950's	Data Processing
960's	Management Reporting
970's	Decision Support
980's	Strategic "
190's onward	E-Business

IS and Business Organization



- Inter organizational factors: Culture, objective, finance, policies etc.
- External organizational factors: Suppliers, Competitors, Government, Consumers

→ Bussiness Processes supported by IS are:

) Operations Support Process

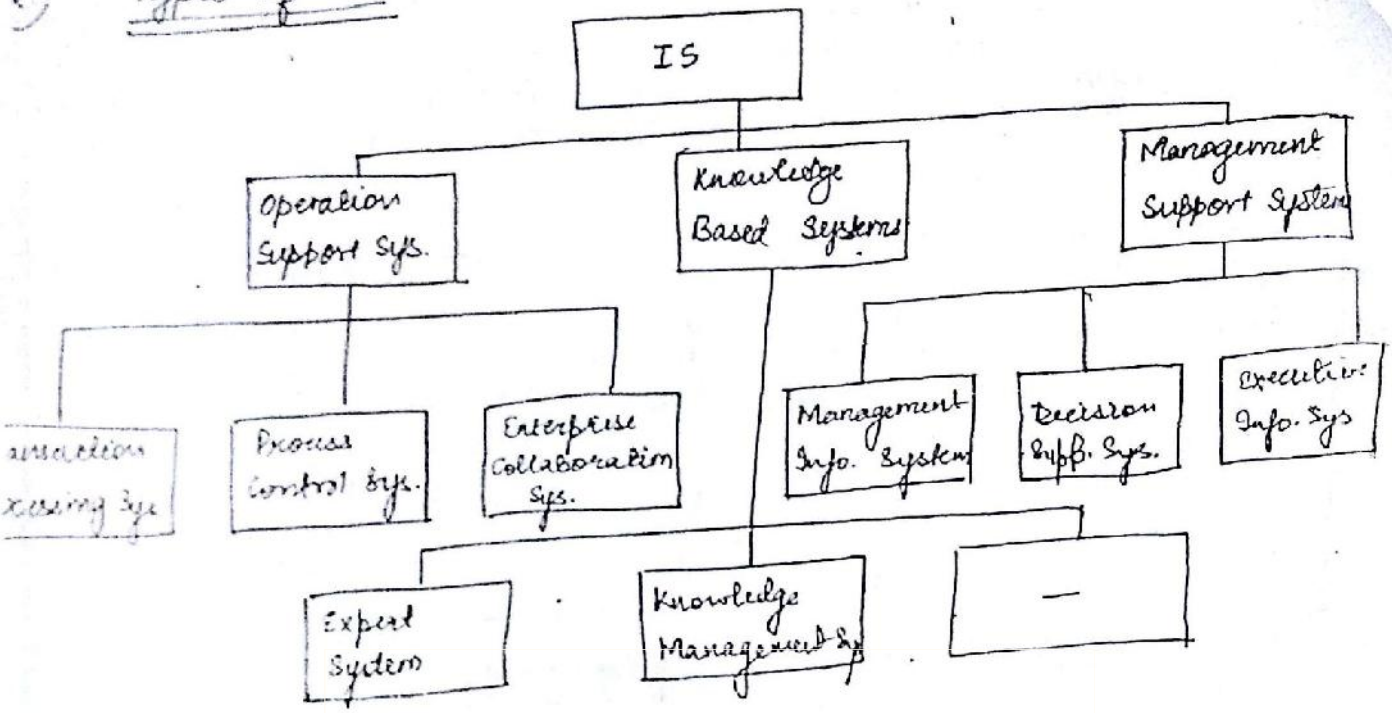
) Decision Support Process – Info. provided after processing data

Strategic Support Process – to gain advantage in competition
eg: Domino's delivery service

IS Failures & Causes

- Incorrect requirement realization
- System Usage
- Poor System Usage
- Other causes.

2) Types of IS



Operation Support System – Supports various business operations such as accounting & production.

i) **Transaction Processing System:** Process business transactions & retrieve info. from them

Batch Processing
(transactions stored over a period of time & then processed)

Online / Real-time processing.
(transactions are processed during their occurrences
ex: retail stores

ii) **Process Control System:** Monitors & control physical processes in an organization.

ex: monitoring pressure in an underground mining plant using electronic sensors to send warnings.

Enterprise Collaboration System : • Sharing information among employees.

• To increase productivity of an organization.

Example : use of electronic mail

Knowledge-Based Systems - provides information → different business areas when required.

i) Expert System : • Adequate knowledge and expert advice for various managerial decisions.

Knowledge base | software modules

management decision making + job related decisions.

ii) Knowledge Management System (KMS) - KMS uses collaboration systems : Intranet

• Provides two types of knowledge — explicit knowledge
— tacit knowledge

• Explicit Knowledge - Info documented, stored & coded with the help of an IS.

• Tacit Knowledge - Info based on processes & procedures stored in human mind.

Management Support Systems - provides information → managers for decision making & control.

Management Information Systems (MIS) : Info on various aspects to

→ generates info for monitoring performance & maintaining coordination

→ Ex: production manager checks report of cost & time production.

Decision Support System (DSS): → supports managerial decision making

→ Ex: sales manager.

Executive Information System (EIS): → provides critical info. to the executive & top managers for making strategic decisions.

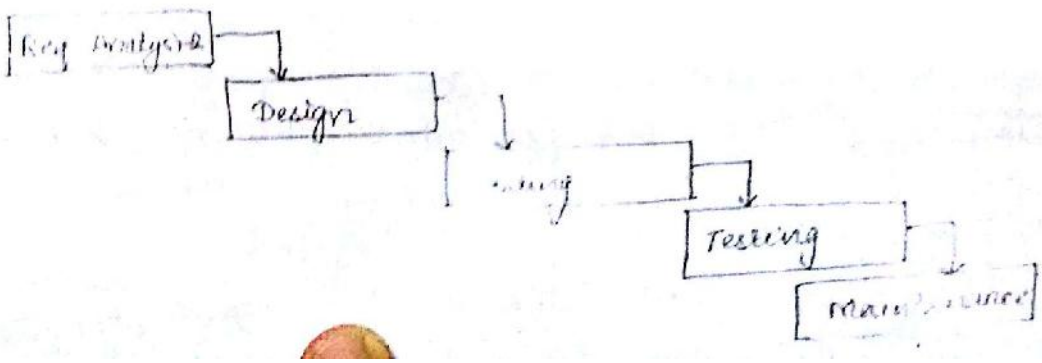
ex: executive checks brand image through graphs.

Development of IS

Suitability of approach — specific i/p conditions
— preference of approach
— development objective

Approaches — Waterfall model
— Prototyping model
— Evolutionary model
— Spiral model
— Interemental model

Waterfall Model — Linear sequential model

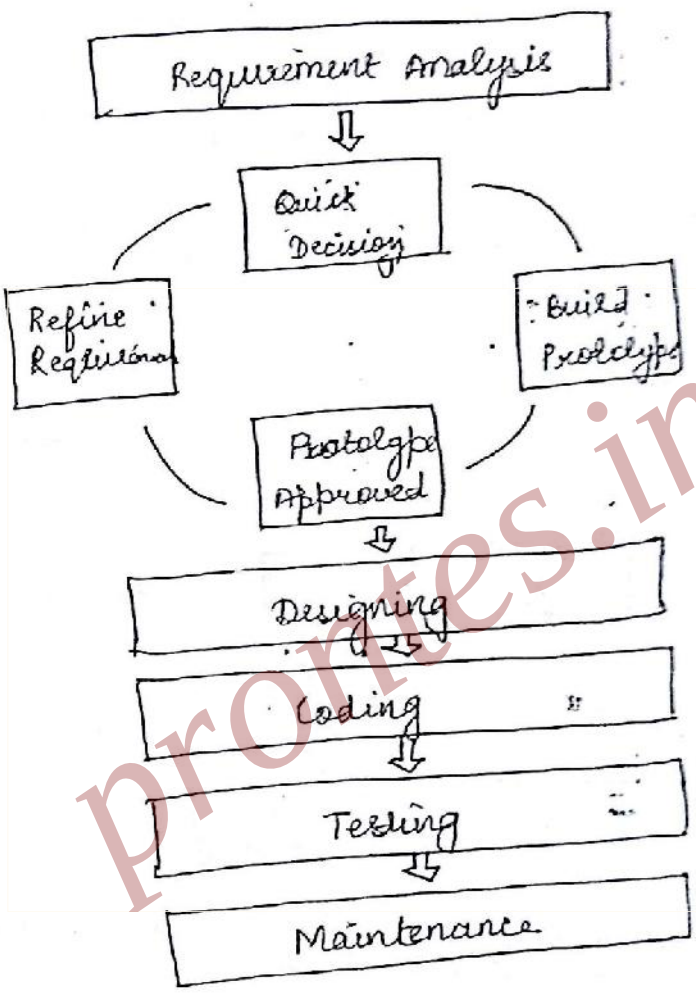


Drawbacks :

Any change in specifications are not possible in later phases.

Feedback about previous process can not be approached.

Prototyping Model (Blueprint of system before actual dev. is prepared).



Prototyping Model to System Development

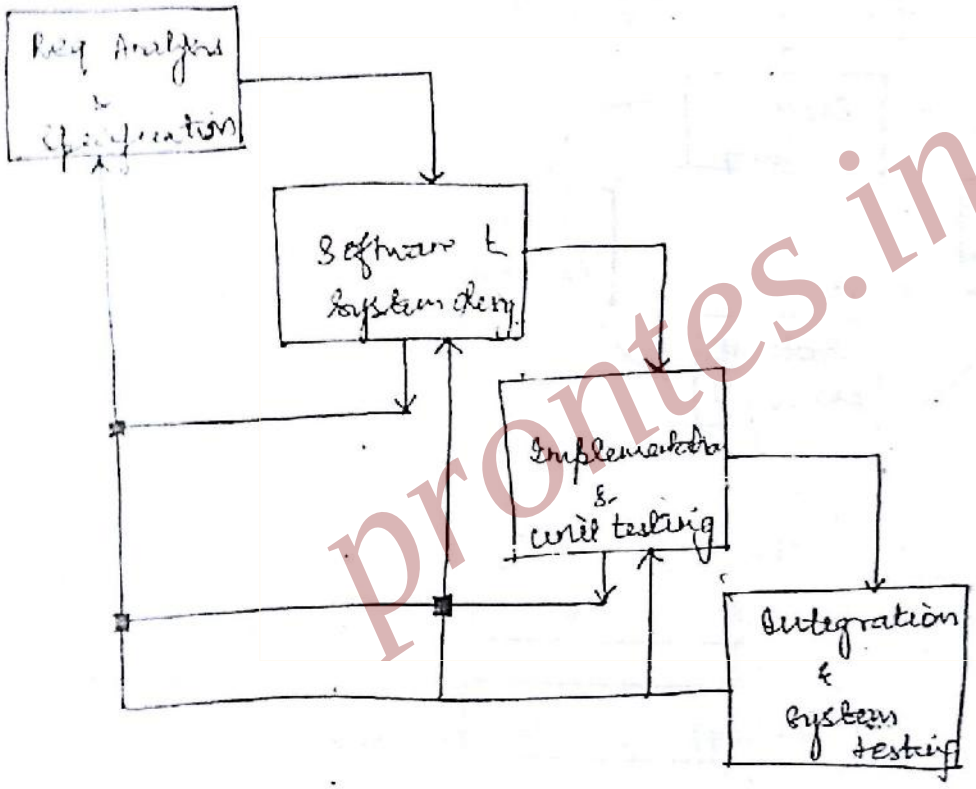
∴ Can trace back the constraints of prototype and improve it

Customer feedback is helpful.

ii) Evolutionary Model : (Improves classic waterfall model).

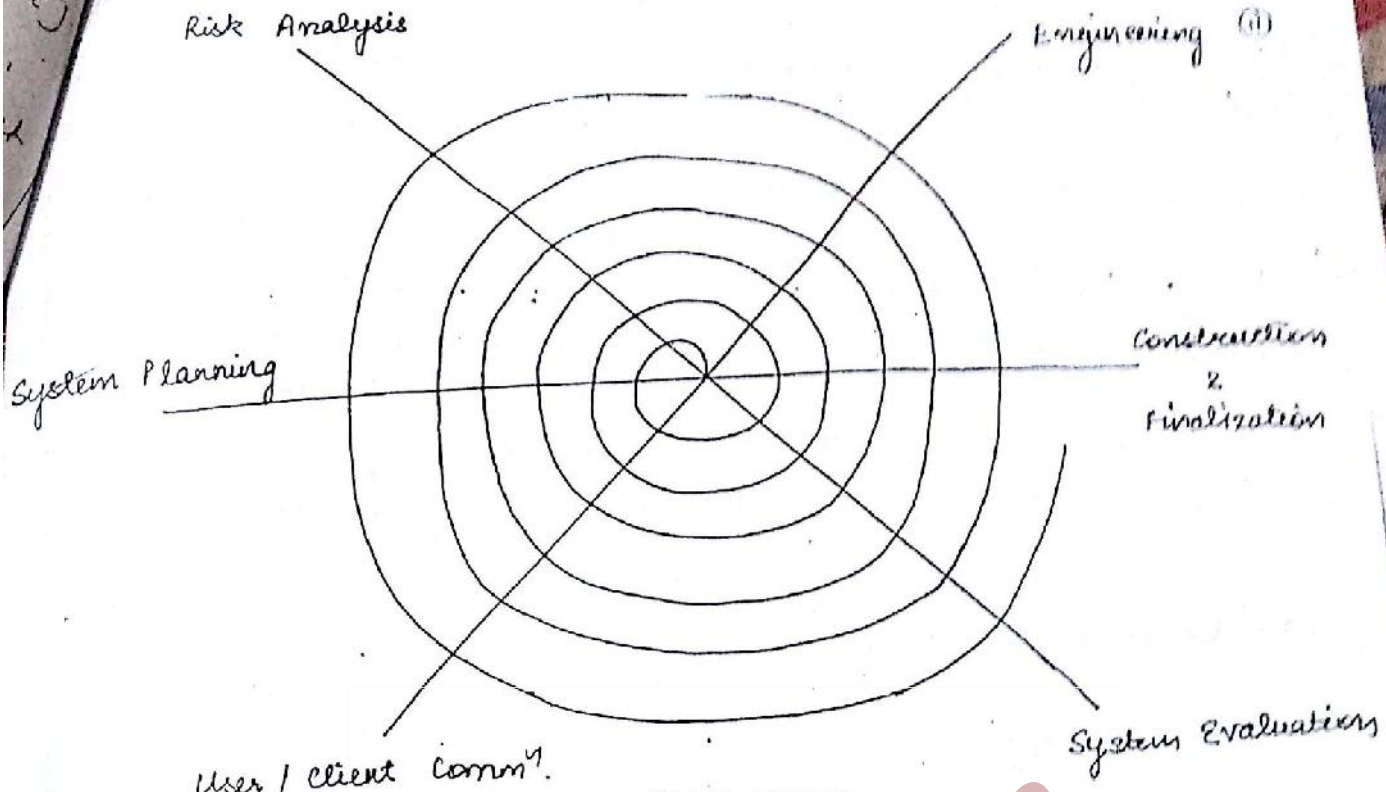
Provides realistic view so that clients can change req. at any stage of system development.

Every stage as seperate evolutionary phase



Evolutionary Approach

Spiral Model : (Combination of features of waterfall & prototype models)



SPIRAL MODEL

Phases of Spiral Model

User / client communication - Interaction with client / users to identify req. & specifications of system

System planning - Rough schema of system & schedule is prepared

Risk Analysis - Identify problems in plan & check for solutions

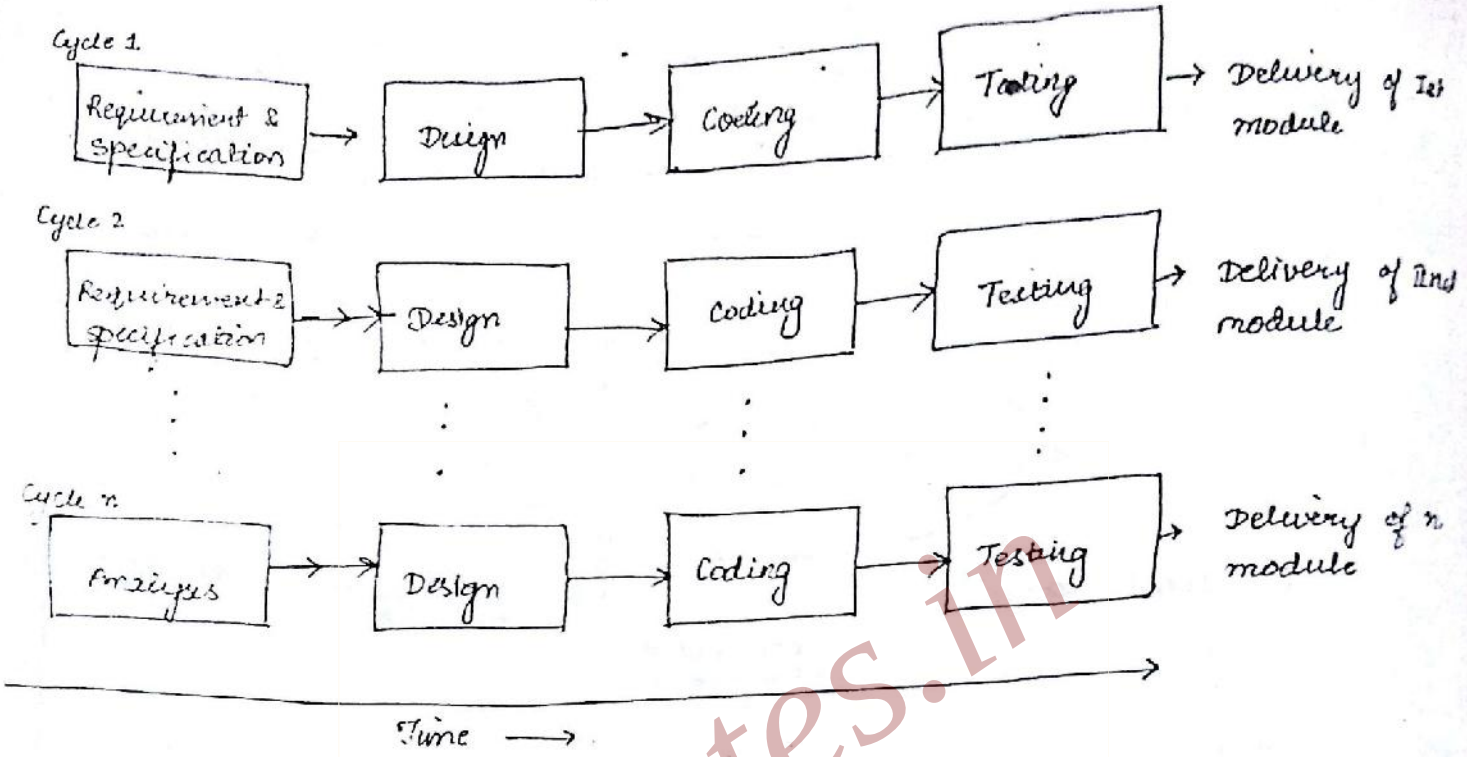
Engineering - System H/W & S/W — Design, Coding & testing the system

Construction & finalization - System build & test to release for use

Evaluation by user / client to use.

System Evaluation -

i) Incremental Model - • Continuous improvement model
• System development to add more functions in process.



Iterative Incremental Model

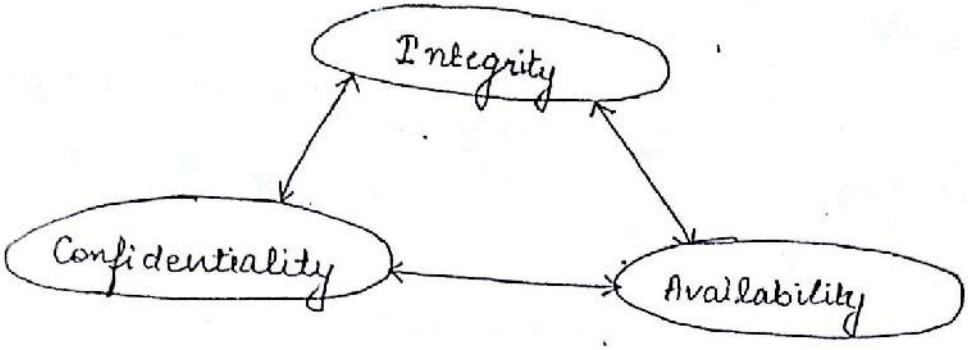
Introduction to Information Security

Information refers to the protection of information

It is the process of securing, protecting and safeguarding the information from unauthorized access, use and modification.

Example: password protection

Key goals: Integrity, Confidentiality and Availability



Relationship between goals of IS

The goals of IS are as follows:

Confidentiality –
- Securing information from unauthorized access
- Only authorized person has right to access the network resources.
- Example: Credit card transaction as credit card number is transmitted over the network in encrypted form

Integrity –
- Accuracy of information or data
- Securing the information from unauthorized modification
- Data can only be modified by authorized user

Availability –
- Information should be available when needed.
- Provided on time
- Fault tolerance exists in the network or computer
- Fair allocation of resources over the network

1 Role of Security in Internet & Web Services

Internet – • Emerging as most widely used medium for performing various tasks such as exchanging data and information
• Conducting online shopping.
• Bank transactions

Security in website is achieved through:

a) Authentication
b) Authorisation

a) Authentication is the process of recognizing the identity of a user.

b) Authorisation is the process of providing the access to the various resources such as databases & printers to authenticated users.

Web Services – • A web service allows a website to communicate with other websites irrespective of programming languages.

Web service complies with common industry standards SOAP & WSDL which allows a website to communicate with other web services irrespective of software and hardware platforms

SOAP - Simple Object Access Protocol

WSDL - Web Services Description Language

Advantages of Web Services

Simple to use on various platforms

Loosely coupled (interface, methods can be extended)

Requests are processed simultaneously.

Security in Web Services

Web Services requests and response are sent as XML documents which are in text format.

Web service from unauthorized access can be prevented by two ways :-

) Encryption and message based security...

Authentication and access controls for the Web service.

Encryption and message based security

Encryption is the process of scrambling the text of web service so that only intended user can decrypt with the help of a key

Message based ... ...ity allows to send encrypted messages ...

by malicious user because the signature attached to message becomes invalid if someone modifies the message.

Security works by encrypting message both at response and request levels.

Authentication and Access Controls for web service

Authentication is the process of validating a user against user credentials given by user.

Access Controls can be done by providing user ID and password. If refused, then access to the web service fails.

Need for Information Security

To maintain proper security of information in an organization application of certain measures, policies and procedures is needed so that no harm is done to confidentiality, integrity and availability of information.

These policies, procedures and standards are included in a system called Information Security Management System (ISMS)

Goal of ISMS :- To remove any possible loss or destruction of information

... network.

Idea : Design, implement & maintain the processes which manages threat to information security in an organization to retain confidentiality, integrity & availability.

Concept : To improve & maintain
- confidentiality
- integrity
- availability

Benefits :
- Protect and secure information in an organization
- Maintains confidentiality, integrity & availability
- Effective organizational management
- Provides high level information security
- Encourages clients and organizations to invest an organization.
- Effectively utilizes data & information.

* Security implication for Organizations

- Security – Process of ensuring the integrity, confidentiality and availability of computer data & resources against viruses, threats and bugs.

- The components of computer where attacker attacks are:
  - Hardware
  - Software
  - Data

- The types of security can be categoised as
  - Computer Security
  - Network Security

Computer Security refers to protection of single / standalone computer.

Network Security refers to protection of computers in the network

Security can be achieved using various methods:

- Identification
- Authentication

Identification is the process of identifying user with user credentials

Authentication is the process of verifying users **authorisation**.

Intrusion Detection System (IDS)

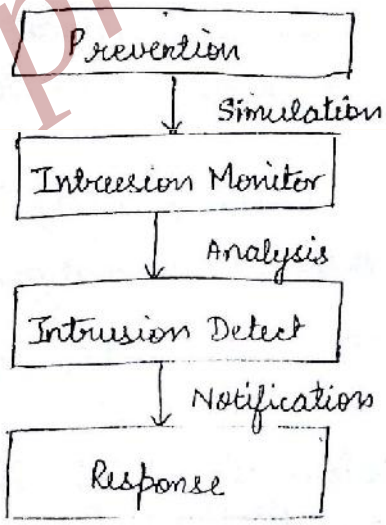
is a system implemented by organizations to protect crucial or confidential data from unauthorized access.

ID monitors network traffic and alerts the system admin of any malicious activity. Example: unauthorised access of data, virus infections etc.

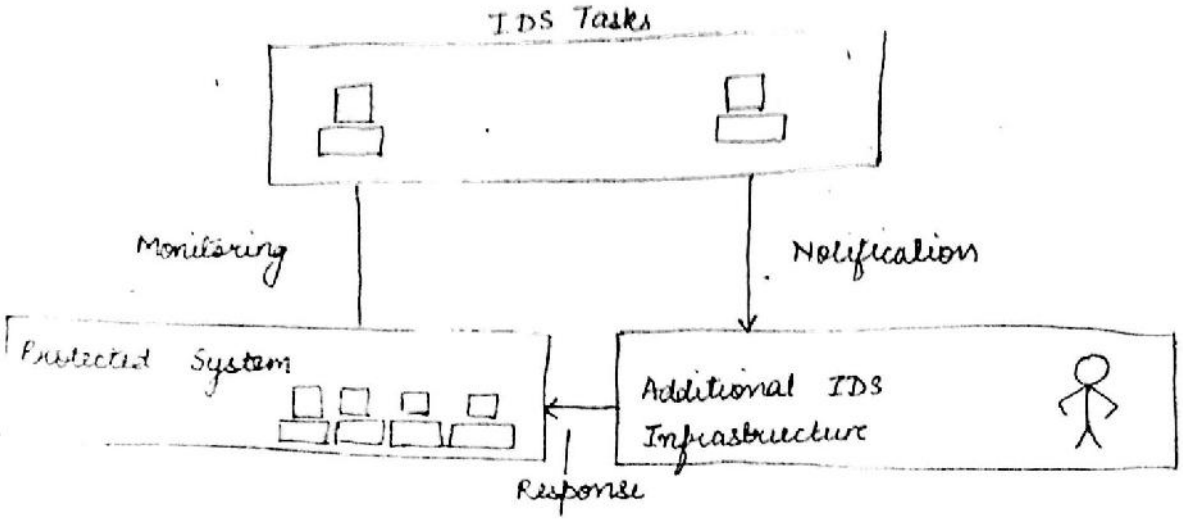
When any such activity is detected ID system blocks source address of user from accessing the network.

Purpose: To provide security from all internal and external intrusions to a system

Working: Scans all information on system or network to which ID is connected to identify security problems such as virus attacks. Blocks or alerts the network administrator about such attacks



Sequence of IDS Activities



Activities of an IDS

Threats to Information Systems

Threat is an illegal activity that can cause damage such as loss of information and data corruption to the network of an organization.

There are two types of threats: Accidental threat and Intentional threat.

Accidental threat is an activity that occurs accidentally and as occurrence is not dependent on any entity.

Intentional threat is an activity that is performed by an entity to violate security of the computer system and network.

Attacks on the network can breach the security of data and resources over the network. There are two types of attacks over the network.

Passive Attack: It is the type of attack in which the attacker does not intend to harm the network. The attacker just monitors, observe or analyse the information available over the network. Example: If aim of attacker is not alteration of messa

Cipher attacks are of 3 types:

Brute force attack: Breaks the encryption of data by finding the appropriate key.

Algebraic attack: Refers to the type of attack in which you can write a cipher as a system equation. After writing a cipher, you can read it by using an appropriate key.

Code book attack: Attacker tries to build a codebook in which he/she describes the cipher text and its corresponding plain text.

Active attack: It is the type of attack in which the attacker intend to attack/harm the network. Also, he/she can modify, edit, delete or manipulate a message.

Information Assurance

IA, according to Information Systems Security Committee (NSTISSC) includes Information Operations (IO) that protect and defend information and informations systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection and reaction capabilities.

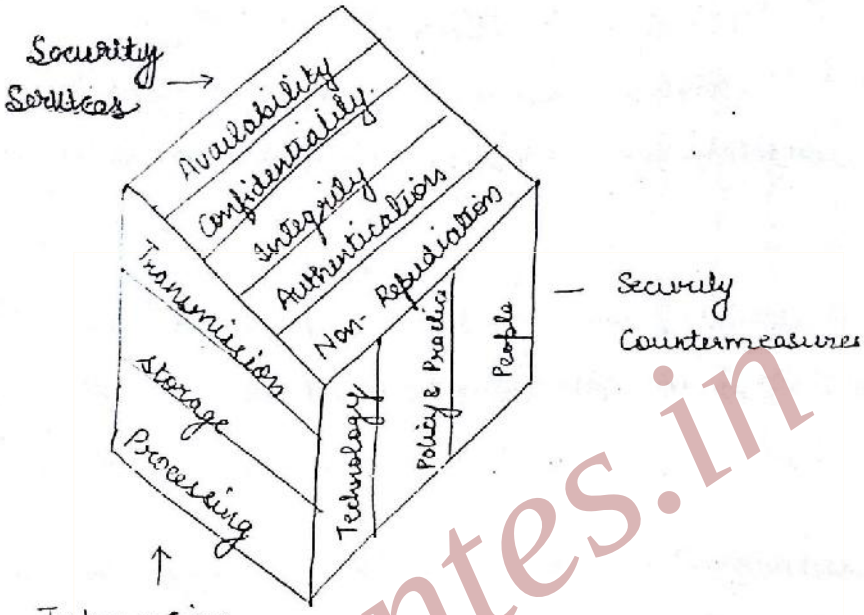
It is related to the management of risks associated with IS of an organization.

It is not a single discipline, it also covers multiple dimensions

The three-dimensional model of IA covers:

) Information states
) Security Measures
) Security Countermeasures

The model of IA is shown as:



Three-D IA Model :-

Information States Information resides in a system in

- Stored form
- processing form
- transmitted form

These three forms are states of information

Ex:- Information that is transmitted is usually stored in disks at sender end Hence information exists in both transmitted and stored states.

Security services: Five essential security services are there:-

Availability - reliable, timely data access facility is available to authorized users.

Confidentiality - Ways to ensure that information is not disclosed.

Integrity - Accurate and complete data or information.

Authentication - Process of identifying and validating the identity of user.

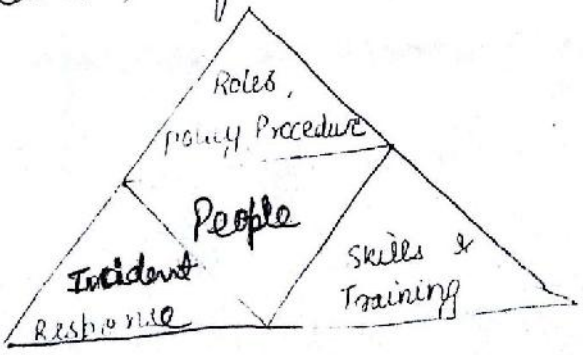
Non-Repudiation - Apply measures through which ownership is not denied for a particular action.

Security Countermeasures: After assessment and analysis of risks, system include countermeasures for maintaining security of IA. These countermeasures are:

Technology - eg. use of cryptography, routers, IDS, firewalls etc.

Operations - application of certain policies, standards and procedures implemented by users and admins of the system.

People - We require awareness, training and education. It is the most significant part of IA as if people concerned with system have no knowledge about security risks and their countermeasures, system can never be totally secure.



Cyber Security

Cyber Security is the protection of information and information security against potential threats on Internet.

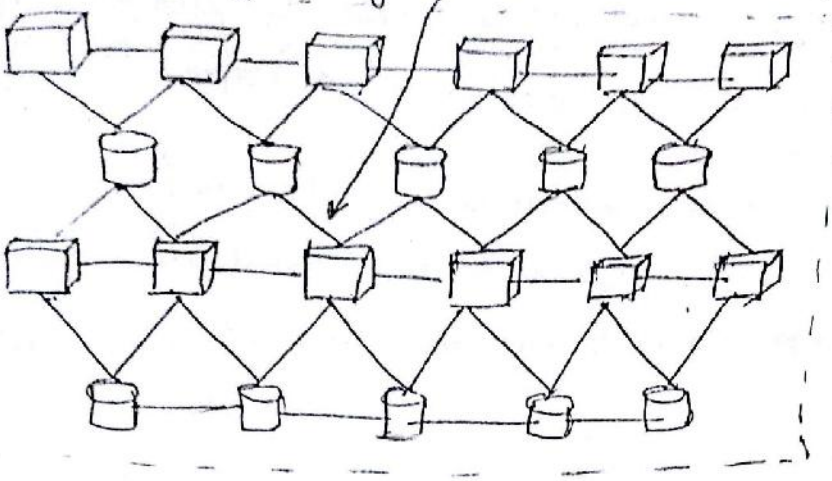
Cyber Security is the ability to protect yourself and your cyberspace (Internet) from the attacks caused through Internet

Difference between IS and Cyber Security

Cyber Security	Information Security
Securing information related to use of internet.	Securing information and information systems against all kinds of unauthorised access, use and modifications
It involves information or information systems	It does not necessarily involves cyberspace.
It is a subset of IS.	It is not a subset of cyber security

Cyber Security is asymmetrical in nature i.e. attacker needs only one single chance to succeed while security manager views system as a whole.

cyber security asymmetry — Attacker need only succeed once!



Showing Cyber Security Asymmetry

Viruses Phishing & Identity Theft

Virus

- A program written to cause harm to a system.
- It can be launched through email & blogposts
- Ex:- sharing information on social networks exchanging emails related to the shared information.

Identity Theft :

- People may steal your identity for criminal purpose which is harmful for victims of identity theft.
- Example : Financial Crime
- One who knows your ATM card PIN and ATM card number might use this sensitive information for his/her benefits

Phishing : An act of convincing people to provide confidential data such as passwords or PINs.

- Example: While downloading application your account password is asked.. If application is not trusted the information may be misused.

Prevention Measures

Use of updated antivirus software and firewalls.

Not installing too many security software programs that may harm your system's performance.

Privacy & security settings of your web browser must not expose your system to potential threat.

Protection for Applications and Individual Privacy

Online advertising can damage an application or send informations from your system to another person who advertises with these programs through use of spyware. This may harm :

Individual privacy

Applications

Prevention Measure
- Keeping check on what you are sharing with whom
- Verifying emails independently and

Keep privacy & security settings of your browser which ask to run or ignore cookies from sites

Be careful while projecting views & giving details about yourself through the Internet.

3 Protection from Online Predator and Cyberbullies

Cyberbullying is the use of internet to stalk other people harass them or extort sexually.

Activities include chatting through mobile applications, consoles of video games, anonymous chat rooms.

Prevention Measure . Guide children of the family, apply a set of rules for children to use Internet safely and giving tips on texting and cyberbullying.

Not tolerating incidents such as exploitation, harassment and stalking.

Security Risk Analysis

Risk Analysis is a process that involves the identification of threats and measuring their effect on the security of an organization.

Process of maintaining organizational security involves
① Assessment ② Analysis (3) management of risks.

) Assessment is identification of any potential risks for a system.

) Analysis means measuring the effects of which can be caused to the system and recording details to the management to take steps for countering.

) Management of risks is taking steps to remove system vulnerabilities.

Risk analysis process acts as a link between risk assessment and risk management processes

Objective : Keeps the economy of a system and security measure to keep it safe and secure in balance

Terminologies of security risk analysis

Assets : Assets for an organization means everything that has some value and needs to be ~~be~~ kept safe.

Threats : Potential actions which can damage the assets of an organization.

Vulnerabilities : Loopholes in securing assets.

Countermeasures : Actions capable to reduce vulnerabilities of system

Expected losses : Expected impact of threats on an organization's assets

Impact: Loss of assets from a threat activity. ex: destruction, modification, disclosure.

Process of risk analysis

Impact Statement: Describes damages that may be caused by threats

Effectiveness measure: Calculated effectiveness of individual actions taken to counter the impact of threats.

Recommended countermeasures: Cost Effective possible actions to maintain security of assets in a proper manner.

xxx