CYBER SECURITY (AUC-002) Syllabus

UNIT-I

Introduction to information systems, Types of information Systems, Development of Information Systems, Introduction to information security, Need for Information security, Threats to Information Systems, Information Assurance, Cyber Security, and Security Risk Analysis.

UNIT-II

Application security (Database, E-mail and Internet), Data Security Considerations-Backups, Archival Storage and Disposal of Data, Security Technology-Firewall and VPNs, Intrusion Detection, Access Control.
Security Threats -Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack, Security Threats to E-Commerce- Electronic Payment System, e-Cash, Credit/Debit Cards. Digital Signature, public Key Cryptography.

UNIT-III

Developing Secure Information Systems, Application Development Security, Information Security Governance & Risk Management, Security Architecture & Design Security Issues in Hardware, Data Storage & Downloadable Devices, Physical Security of IT Assets, Access Control, CCTV and intrusion Detection Systems, Backup Security Measures.

UNIT-IV

Security Policies, Why Policies should be developed, WWW policies, Email Security policies, Policy Review Process-Corporate policies-Sample Security Policies, Publishing and Notification Requirement of the Policies.
Information Security Standards-ISO, IT Act, Copyright Act, Patent Law, IPR. Cyber Laws in India; IT Act 2000 Provisions, Intellectual Property Law: Copy Right Law, Software License, Semiconductor Law and Patent Law.

References:

1. Charles P. Pfleeger, Shari Lawerance Pfleeger, "Analysing Computer Security", Pearson Education India.

2.V.K. Pachghare, "Cryptography and information Security", PHI Learning Private Limited, Delhi India.

3. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen kumar Shukla ,"Introduction to Information Security andCyber Law"Willey Dreamtech Press.

4. Schou, Shoemaker, "Information Assurance for the Enterprise", Tata McGraw Hill.

Introduction to Information Systems

What is data?

Data consist of raw facts or stream of things that are happening now and have happened in the past.

What is information?

Information is data that has been transformed into a more useful form. It's important to say that information have a value.

What is knowledge?

Knowledge is the stock of conceptual tools and categories used by humans to create, collect store, and share information.

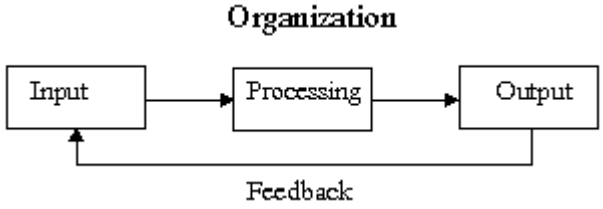
What is a system?

A **system** is a set of elements with relationships between them. They work together to achieve a common purpose or goal. System has inputs, processing mechanisms and outputs.

Systems can be relatively simple, or they can be more complex. Hospitals, manufacturers, insurance companies and electric utilities can be viewed as systems. In most of these cases, the system goals is profit maximization or customer satisfaction. Inputs of these systems include labor, capital, land, merchandise, equipment, and so on. Output from these systems is the goods and services offered by the business. The system boundary defines the system and distintinguishes it from everything else. The input, the processing mechanism and the output are system elements.

What is an information system?

Information system is a set of interrelated elements or components that collect (input), manipulate and store (processing), and disseminate (output) data and information as well as feedback mechanism.



Input is the activity of capturing raw data resources in the organization.

Processing involves converting (as calculations, comparisons and storing) this raw input into a more appropriate

and useful outputs.

Output involves producing useful information to the people or activities that will use it in the form of documents or reports.

Feedback is used to refine or to correct the input raw. Feedback is also important for managers and decision makers.

Component of Information systems:-

An information system is a product of three components: technology, organizations and people. To use IS effectively and efficiently in a business it is needed also to understand the problems faced by organizations, the proposed architectural and aesthetic solutions and the organizational process that leads to the systems.

External Environment includes political, demographic, economic and social trends.

Organizations as a system can be measured in terms of efficiency (is a measure of the extent to which a system achieves its goals) and effectiveness (is a measure of what is produced devided by what is consumed). Organization structure refers to organizational subunits are related as system elements. It is hierarchical and structured. Employees are arranged in a rising levels of authority. The upper levels of the hierarchy consist of management, and the lower levels consist of non-managerial employees. Formal rules, methods or

procedures for accomplishing tasks (such as how to write up a purchase order or how to correct an erroneous bill), are used to coordinate specialized groups in the firms so they will complete their work in an acceptable manner.

People are most important element in most CBIS. IS include all people who manage, run, and maintain the computer system. Their knowledge and qualification can increase to use more Information systems and to apply into their jobs more efficiently and effectively.

The Technology transforms and organizes data into useful form. There are two related technology problems: (1) computing software is changing more rapidly than ability to buy appropriate hardware; (2) organizations cannot to apply changes of hardware and software.

Computer hardware consists of any machinery that assist the performance of the input, processing and output activities of an information systems.

Computer software is a set of instructions that controls hardware to perform processing of information systems.

The storage technology is a powerful determinant of the data usefulness and availability in a business.

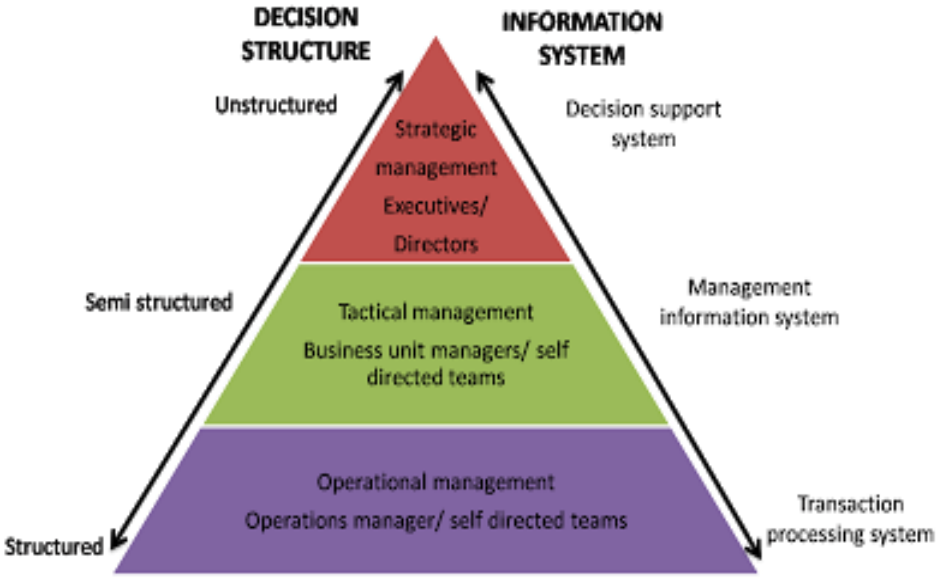
Telecommunication technology is used to link different pieces of hardware and to transfer data from one location to another. It's involves physical media and software that support communication by electronic mean, usually over come distance.

Knowledge about information technology - computer hardware, computer software, storage and techniques are computer literacy**.**

Information systems literacy is is knowledge of how data information are used by individuals and organizations. It consists of three elements:

- Information Technology Skills
- Analysis and Problem-Solving Skills
- Organizational and Individual Behavior Skills

TYPES OF INFORMATION SYSTEM:-



Information systems differ in their business needs and the information varies depending upon different levels in organization. Information system can be broadly categorized into following:

- Transaction processing system
- Management Information System
- Decision support system

The information needs are different at different organizational levels. Accordingly the information can be categorized into following:

- Strategic information
- Managerial information
- Operational information.

Transaction Processing Systems

1. It processes business transaction of the organization. Transaction can be any activity of the organization. For example, take a railway reservation system. Booking, canceling, etc are all transactions. Any query made to it is a transaction.
2. This provides high speed and accurate processing of record keeping of basic operational processes and include calculation, storage and retrieval.
3. Transaction processing systems provide speed and accuracy, and can be programmed to follow routines functions of the organization.

Management Information Systems

1. It assist lower management in problem solving and making decisions. They use the results of transaction processing and some other information also.
2. An important element of MIS is database. A database is a non-redundant collection of interrelated data items that can be processed through application programs and available to many users.

Decision Support Systems

1. These systems assist higher management to make long term decisions. These type of systems handle unstructured or semi structured decisions. A decision is considered unstructured if there are no clear procedures for making the decision and if not all the factors to be considered in the decision can be readily identified in advance.
2. A decision support system must very flexible.
3. The user should be able to produce customized reports by giving particular data and format specific to particular situations.

Different software life cycle models

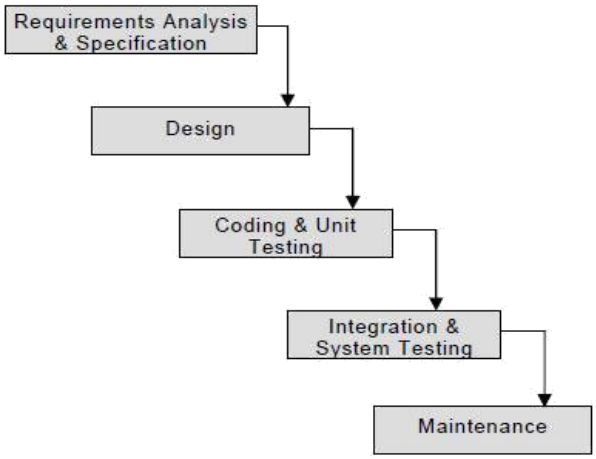
Many life cycle models have been proposed so far. Each of them has some advantages as well as some disadvantages. A few important and commonly used life cycle models are as follows:

1. Classical Waterfall Model
2. Iterative Waterfall Model
3. Prototyping Model
4. Evolutionary Model
5. Spiral Model

Classical Waterfall Model:-

The classical waterfall model is intuitively the most obvious way to develop software. Though the classical waterfall model is elegant and intuitively obvious, it is not a practical model in the sense t hat it cannot be used in actual software development projects. Thus, this model can be considered to be a theoretical way of developing software. But all other life cycle models are essentially derived from the classical waterfall model. So, in order to be able to appreciate other life cycle models it is necessary to learn the classical waterfall model.
Classical waterfall model divides the life cycle into the following phases as shown in fig:

1. Feasibility Study
2. Requirements Analysis and Specification
3. Design
4. Coding and Unit Testing
5. Integration and System Testing
6. Maintenance

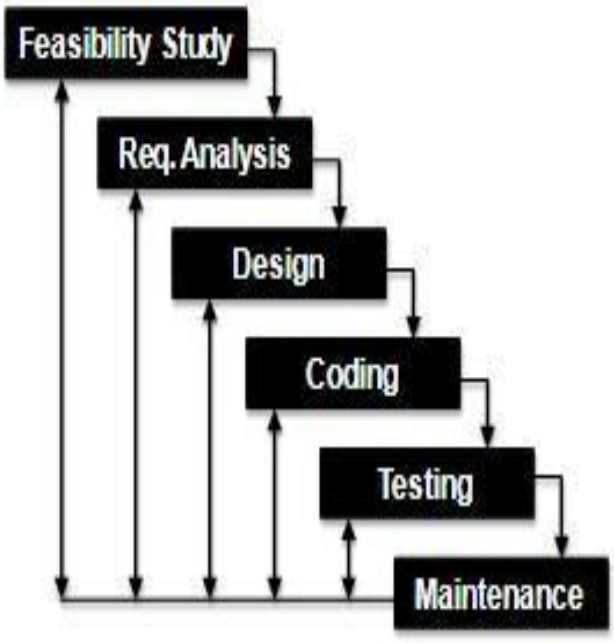


Classical Waterfall Model

Iterative Waterfall Model:-

- Waterfall model assumes in its design that no error will occur during the design phase
- Iterative waterfall model introduces feedback paths to the previous phases for each process phase
- It is still preferred to detect the errors in the same phase they occur
- Conduct reviews after each milestone

S



Iterative Waterfall Model

Advantages of Waterfall Model

- It is a linear model.
- It is a segmental model.
- It is systematic and sequential.
- It is a simple one.
- It has proper documentation

Disadvantages of Waterfall Model

It is difficult to define all requirements at the beginning of the project.

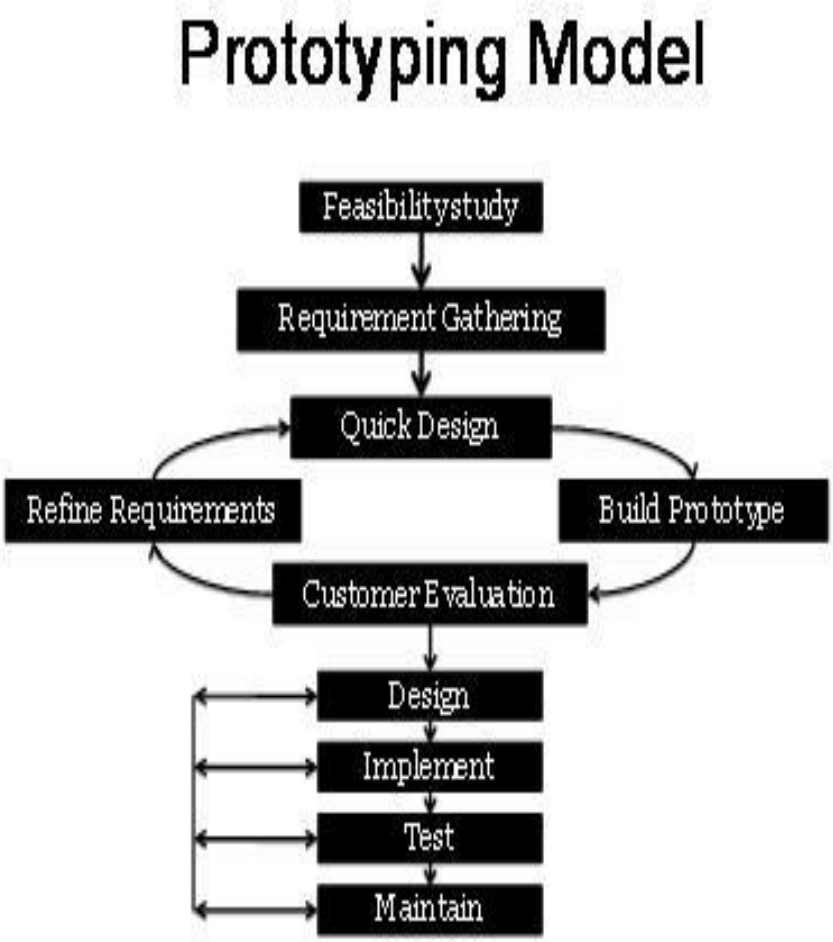
- Model is not suitable for accommodating any change
- It does not scale up well to large projects
- Inflexible partitioning of the project into distinct stages makes it difficult to respond to changing customer requirements.
- Therefore, this model is only appropriate when the requirements are well-understood and changes will be fairly limited during the design process.
- Few business systems have stable requirements.
- The waterfall model is mostly used for large systems engineering projects where a system is developed at several sites.

Prototype model:-

The Prototyping Model is a systems development method (SDM) in which a prototype is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved from which the complete system or product can now be developed prototyping paradigm begins with requirements gathering.

- Developer and customer meet and define the overall objectives for the software, identify whatever requirements are known, and outline areas where further definition is mandatory.
- A "quick design" then occurs. The quick design focuses on a representation of those aspects of the software that will be visible to the customer/user (e.g., input approaches and output formats).

There are several steps in the Prototyping Model as shown in the diagram:-



A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product

1. The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the departments or aspects of the existing system.
2. A preliminary design is created for the new system.

.

3. The users thoroughly evaluate the first prototype, noting its strengths and weaknesses, what needs to be added, and what should to be removed. The developer collects and analyzes the remarks from the users.
4. The first prototype is modified, based on the comments supplied by the users, and a second prototype of the new system is constructed.
5. The second prototype is evaluated in the same manner as was the first prototype.
6. The preceding steps are iterated as many times as necessary, until the users are satisfied that the prototype represents the final product desired.
7. The final system is constructed, based on the final prototype.
8. The final system is thoroughly evaluated and tested. Routine maintenance is carried out on a continuing basis to prevent large-scale failures and to minimize downtime.

Customers could believe it's the working system. Developer could take "shortcuts" and only fill the prototype instead of redesigning it. Customers may think that the system is almost done, and only few fixes are needed

Advantage of Prototype model

- Suitable for large systems for which there is no manual process to define there requirements.
- User training to use the system.
- User services determination.
- System training.
- Quality of software is good.
- Requirements are not free zed.

Disadvantage of Prototype model

- It is difficult to find all the requirements of the software initially.
- It is very difficult to predict how the system will work after development.

Evolutionary Process Model:-

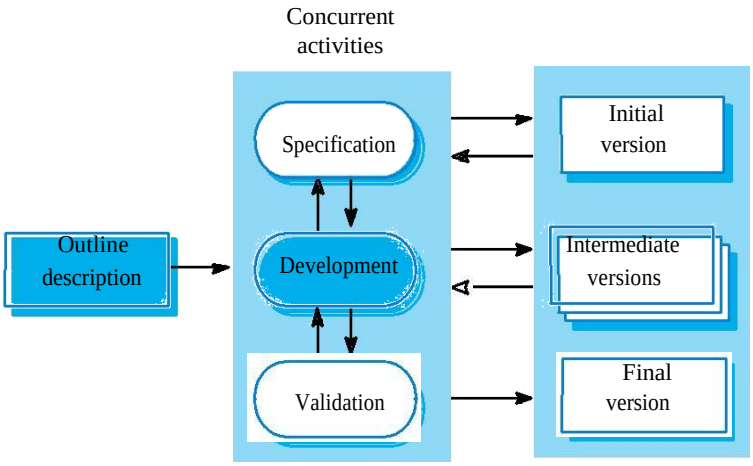
In EP model development engineering effort is made first to establish correct, precise requirement definitions and system scope, as agreed by all the users across the organization? This is achieved through application of iterative processes to evolve a system most suited to the given circumstances.

The process is iterative as the software engineer goes through a repetitive process of requirement until all users and stakeholders are satisfied. This model differs from the iterative enhancement model in the sense that this does not require a useable product at the end of each cycle. In evolutionary development, requirements are implemented by category rather than by priority.

Main characteristics:

– The phases of the software construction are interleaved
– Feedback from the user is used throughout the entire process
– The software product is refined through many versions

- Types of evolutionary development:
  – Exploratory development
  – Throw-away prototyping



Advantages:

- Deals constantly with changes
- Provides quickly an initial version of the system
- Involves all development teams

Disadvantages:

- Quick fixes may be involved
- "Invisible" process, not well-supported by documentation
- The system's structure can be corrupted by continuous change

Spiral model

The Spiral model of software development is shown in fig. The diagrammatic representation of this model appears like a spiral with many loops. The exact number of loops in the spiral is not fixed. Each loop of the spiral represents a phase of the software process. For ex ample, the innermost loop might be concerned with feasibility study. The next loop with requirements specification, the next one with design, and so on. Each phase in this model is split into four sectors (or quadrants) as shown in fig.

The following activities are carried out during each phase of a spiral model.

First quadrant (Objective Setting)

- During the first quadrant, it is n eeded to identify the objectives of the phase.
- Examine the risks associated with these objectives.

Second Quadrant (Risk Assessment and Reduction)

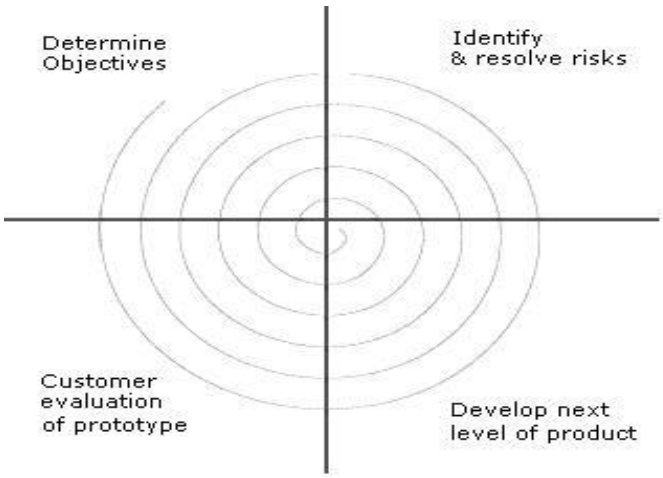
- A detailed analysis is carried out for each identified project risk.
- Steps are taken to reduce the risks. For example, if there is a risk that the requirements are inappropriate, a prototype system may be developed.

Third Quadrant (Development and Validation)

- Develop and validate the next level of the product after resolving the identified risks.

Fourth Quadrant (Review and Planning)

- Review the results achieved so far with the customer and plan the next iteration around the spiral.
- Progressively more complete version of the software gets built with each iteration around the spiral.



Advantages of Spiral Model

- It is risk-driven model.
- It is very flexible.
- Less documentation is needed.
- It uses prototyping

Disadvantages of Spiral Model

- No strict standards for software development.
- No particular beginning or end of a particular phase.

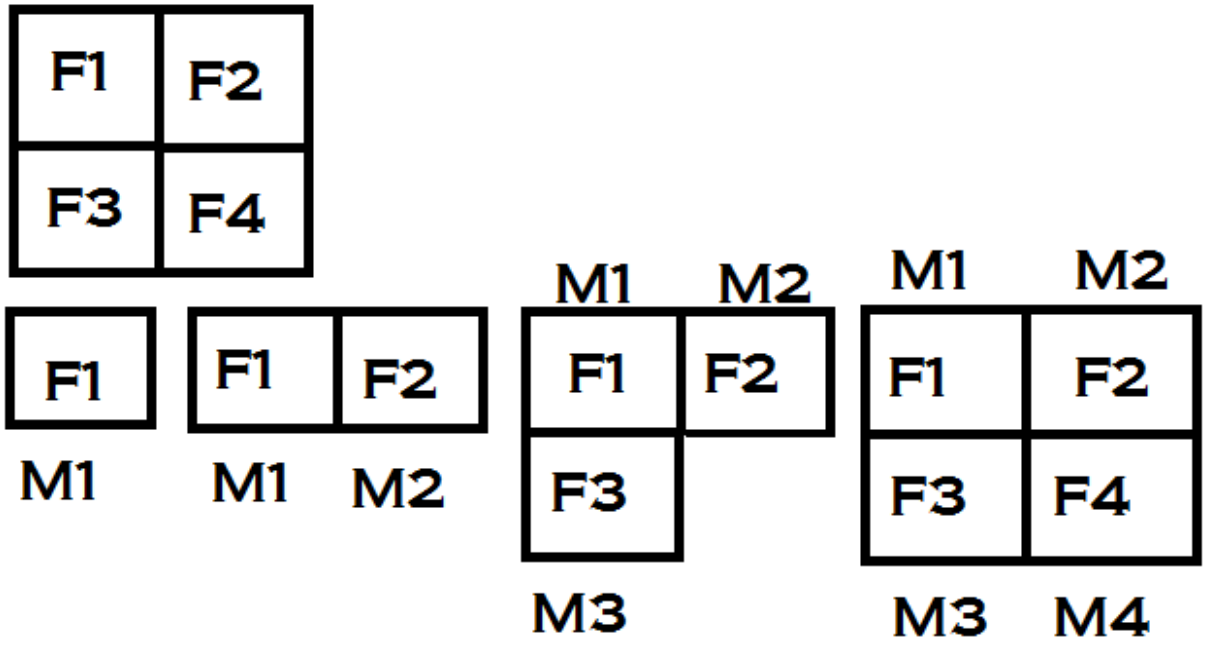
Difference between spiral and waterfall model

Waterfall model	Spiral model
Separate and distinct phases of specification and development.	Process is represented as a spiral rather than as a sequence of activities with backtracking
After every cycle a useable product is given to the customer.	Each loop in the spiral represents a phase in the process
Effective in the situations where requirements are defined precisely and there is no confusion about the functionality of the final product.	No fixed phases such as specification or design - loops in the spiral are chosen depending on what is required
Risks are never explicitly assessed and resolved throughout the process	Risks are explicitly assessed and resolved throughout the process

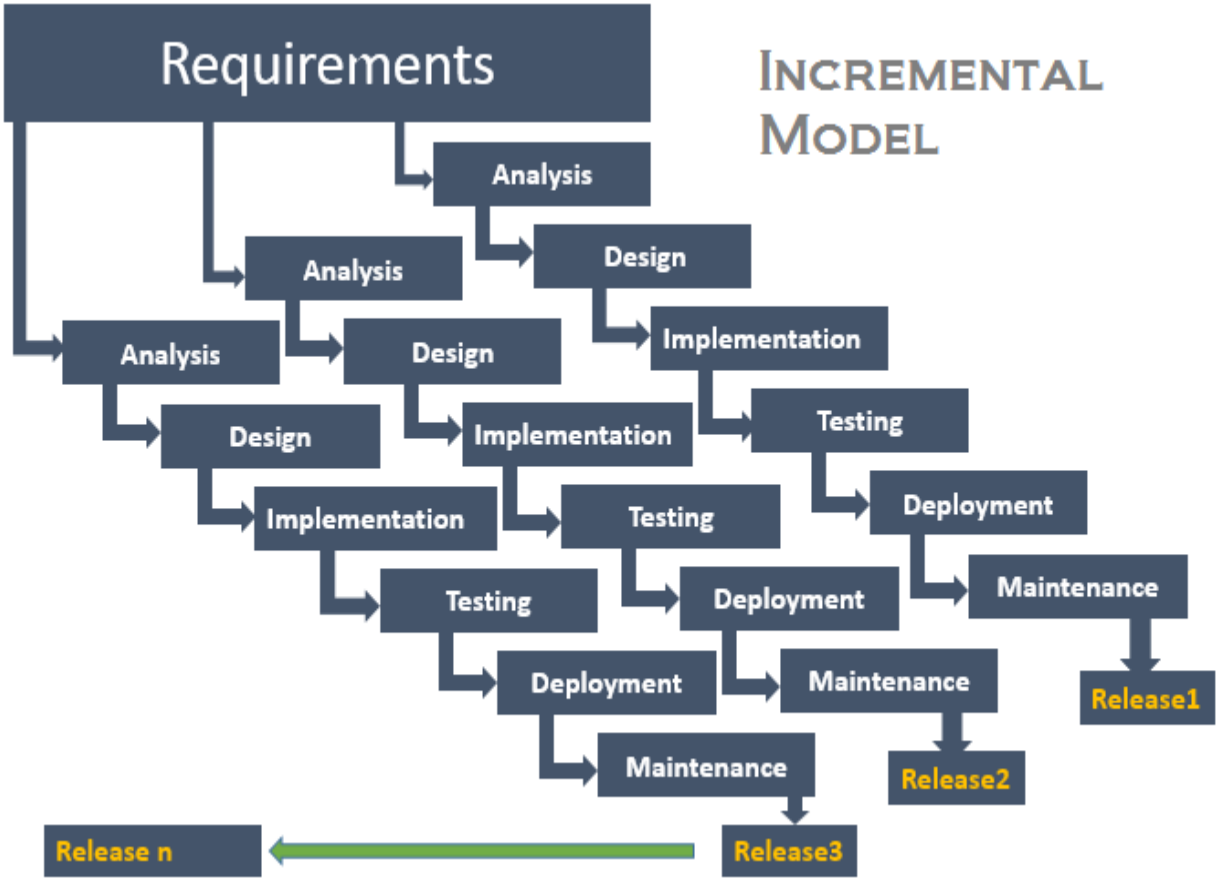
Incremental Model:-

Incremental Model is combination of one or more Waterfall Models. In Incremental Model, Project requirements are divided into multiple modules and each module is developed separately. Finally developed modules are integrated with other modules. During development of each module, waterfall model is followed for each module development separately. Each developed module in Incremental Model is standalone feature and could be delivered to the end users to use it. On incremental basis other modules are integrated as additional features one after another and finally delivered to the client. In Incremental Model no need to wait for all the modules to be developed and integrated. As each module is standalone application and there is no dependencies on other modules so we can deliver the project with initial developed feature and other features could be added on incremental basis with new releases. Incremental process goes until all the requirements fulfilled and whole system gets developed.

Example-1:



Consider in the above picture, there is one square that has to develop with features F1, F2, F3 and F4. In the Incremental Model all the four features will be divided into four different small squares called modules (M1, M2, M3 and M4).Once the first module (M1) is developed, it gets delivered to the client and later on after development of second module M2 integrated with module M1. Gradually we develop other modules M3 and M4 and keep on integrating until complete square gets ready or developed.



Incremental Model helps to deliver the sequence of releases in incremental basis which speeds up the progress of development of each functionality. Each developed functionality gets delivered to the end users one after another. First increment is always a base feature and other features added in next increments with new releases in

case client requests to add the any new feature after review of first release. This process is carried out till the complete product developed.

Advantages of Incremental Model

- **Generates working software quickly and early during the software life cycle.**
- **More flexible – less costly to change scope and requirements.**
- **Easier to test and debug during a smaller iteration.**
- **Easier to manage risk.**

Disadvantages of Incremental Model

- **Each phase of an iteration is rigid and do not overlap each other.**
- **Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.**

Introduction to information security:-

Confidentiality: Ensures that the information in a computer system a n d transmitted Information are accessible only for reading by authorized parties.
E.g. Printing, displaying and other forms of disclosure.
Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
Availability: Requires that computer system assets be available to authorized parties when needed.

Need for Information security:

Because we want in the organization there is no harm is caused to the confidentiality, integrity, availability. Information security performs four important functions for an organization:

1. Protecting the Ability to Function:
2. Enable Safe Operation
3. Protecting Data
4. Safeguarding Technology Assets

Threats to Information Systems:-

Active attacks: These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity.

Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Passive Attacks:-

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing

the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Information Assurance:-

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
E.g. Printing, displaying and other forms of disclosure.
Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Availability: Requires that computer system assets be available to authorized parties when needed.

Cyber Security:

Cyber security, also referred to as information technology security, focuses on

protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

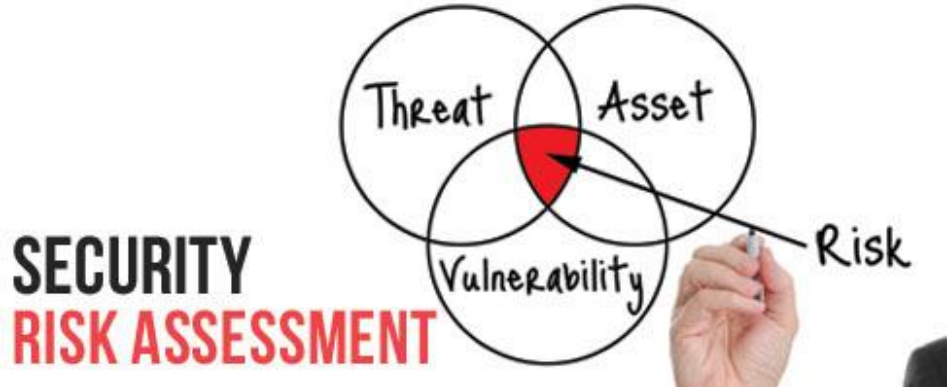
During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism.

Security Risk Analysis:

Risk analysis is the process of evaluating system vulnerabilities and threats facing it. A risk analysis is the process of identifying the assets you wish to protect and the potential threats against them.

Risk Analysis Terminology

1. **Assets:** Anything with value and in need of protection.
2. **Threat:** An action having possibility of damage.
3. **Vulnerability:** A condition of weakness.
4. **Countermeasure:** An action with the ability to reduce vulnerability.
5. **Expected Loss:** The negative impact to assets due to threat. Four areas are commonly used:
    - Destruction
    - Denial of services
    - Disclosure
    - Modification.



The process of risk analysis involves the following three elements:

1. **Impact statement:** describe the damages by threat.
2. **Effectiveness measures:** calculating of individual action taken by threat.
3. **Recommended countermeasure:** series of recommendations to correct or minimize Identified problems.