

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are highlighted with blue circles, and others with blue dots. The lines are thin and grey, creating a mesh-like structure.

Unit-1

Information System

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with several nodes highlighted in blue.

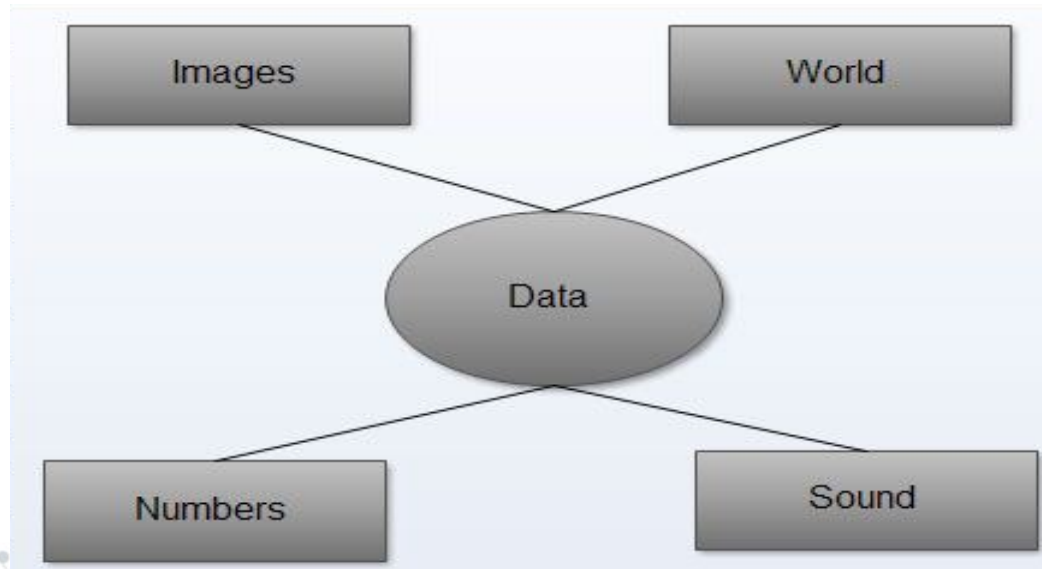
Index

- Information System
- Types of Information System
- Development Information System
- Information Security
- Need of Information Security
- Threats to Information Security
- Information Assurance
- Cyber Security and Risk Analysis

Data

- Data is the raw material that can be processed by any computing machine.
Data can be represented in the form of:
- Numbers and words which can be stored in computer's language, Images, sounds, multimedia and animated data as shown

Data can be anything...



INFORMATION

- Information is data that has been converted into a more useful or intelligible form. It is the set of data that has been organized for direct utilization of mankind, as information helps human beings in their decision making process.

OR

- Information is data that has been processed in such a way as to be meaningful to the person who receives it. it is any thing that is communicated.



Need of Information

- To gain knowledge about the surroundings, and whatever is happening in the society and universe.
- To keep the system up to date.
- To know about the rules and regulations and bye laws of society, local government, and central government, associations, clients etc. as ignorance is no bliss.
- Based on above three, to arrive at a particular decision for planning current and prospective actions in process of forming, running and protecting a process or system

Information System

Information systems are collections of multiple information resources to gather, process, store, and disseminate information.

e.g., software, hardware, computer system connections, the system housing, system users, and computer system information





Any Organized combination of :

- People
- Hardware
- Communication network
- Software
- Data resources
- Policies and procedures



Note: Companies and organizations employ information systems to communicate and work with their customers and suppliers, manage the organization, perform essential business operations, and roll out and maintain marketing campaigns.

Components of Information System:-

There are various components of an information system:

1. Hardware
2. Software
3. Data
4. Telecommunications
5. People



Components of Information Systems

Hardware

- The hardware component of an information system comprises the physical elements of the system.
- People can touch and feel pieces of hardware.
- These mechanisms, equipment and wiring allow systems like computers, smartphones and tablets to function.
- Input and output devices are essential pieces of technology that allow humans to interact with computers and other information systems.
- Keyboards, mice, microphones and scanners are all examples of input devices. And output devices might include printers, monitors, speakers and sound and video cards.
- Pieces of hardware including microprocessors, hard drives, electric power supply units, and removable storage also allow computers to store and process data.

Software

- Software are the intangible programs that manage information system functions, including input, output, processing and storage.
- System software – such as the MacOS or Microsoft Windows operating systems – provides a base for application software to run.
- Application software operates programs geared toward particular uses in information systems.
- Graphical user interface (GUI) software is among the most common application software. it presents the information stored in computers and allows users to interact with computers through digital graphics – such as icons, buttons and scroll bars – rather than through text-based commands.

Data

- Data are intangible, raw facts that are stored, transmitted, analyzed and processed by other components of information systems.
- Data are often stored as numerical facts, and they represent quantitative or qualitative information.
- Data can be stored in a database or data warehouse, in a form that best suits the organization using it.
- Databases house collections of data that can be queried or retrieved for specific purposes.
- Databases allow users to perform fundamental operations, such as storage and retrieval.
- Data warehouses, on the other hand, store data from multiple sources for analytical purposes.
- They allow users to assess an organization or its operations.

Telecommunications

- Telecommunications systems connect computer networks and allow information to be transmitted through them.
- Telecommunications networks also allow computers and storage services to access information from the cloud.
- Local-area networks (LANs) connect computers to create computer networks in a designated space, like a school or home.
- Wide-area networks (WANs) are collections of LANs that facilitate data-sharing across large areas.
- A virtual private network (VPN) allows a user to protect their online privacy by encrypting data on public networks.
- Microwaves and radio waves can also be used to transmit information in telecommunications networks.



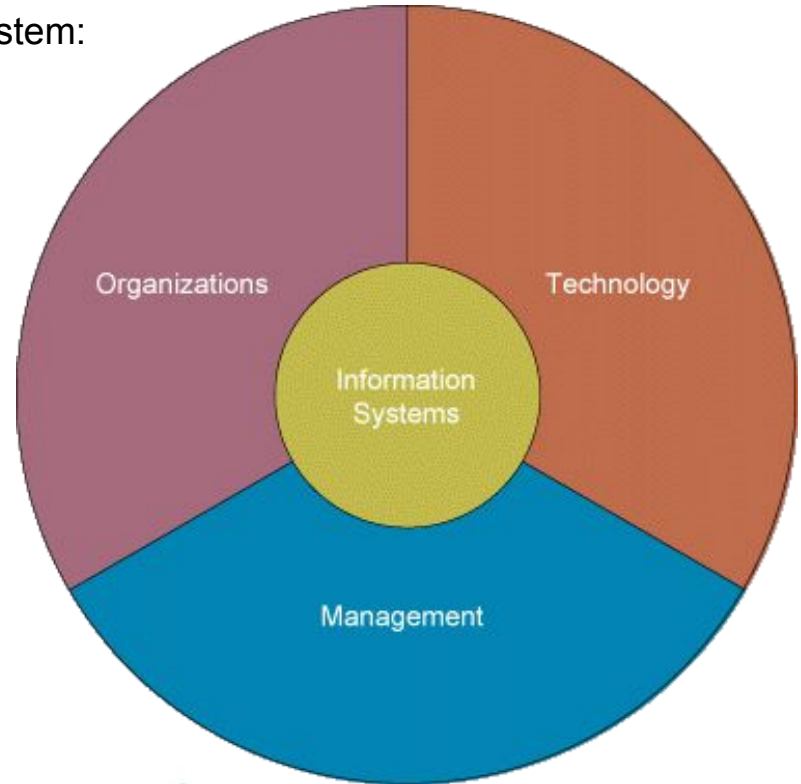
Human Resources

- Human resources are a crucial part of information systems.
- The human component of information systems encompasses the qualified people who influence and manipulate the data, software and processes in information systems.
- Humans involved in information systems may include business analysts, information security analysts or system analysts.
- Business analysts work to elevate an organization's operations and processes. They often focus on improving efficiency and productivity or streamlining distribution.
- Information security analysts work to prevent data breaches and cybersecurity attacks. And system analysts use information technology to help organizations optimize their user experiences with programs.

Dimensions of an information system

There are main three dimensions of an information system:

1. Organisationnel dimension
2. Management dimension
3. Technologie dimension






Organizational Dimension

The information system is the organization's part. The ordinary operating procedure and culture of an organization would be embedded in the information system.

This includes the following:

- Business processes
 - Political interest groups
 - Functional specialties
 - Cultured
- 



Management Dimension

Information systems provide managers with the tools and information they have to plan, manage, monitor their work, make decisions, develop new goods and services, and make long-term tactical decisions.

Technology Dimension

Management makes use of technology to fulfill their duties.

It contains- computer hardware and software, networking/telecom technology, and data management.

It's one of the many strategies a manager can use to deal with changes.

Organizational levels, processing, system goals, mode of data and type of support provided are used to classify information systems.

Types of Information System

1. Transaction Processing System // Operations support systems
2. Management information systems
3. Decision support systems
4. Executive information systems // Expert information system

Types of Information System



Transaction Processing System (TPS)

- Transaction Processing System are information system that processes data resulting from the occurrences of business transactions
- Their objectives are to provide transaction in order to update records and generate reports.

The transaction is performed in two ways:

1. Batching processing
2. Online transaction processing

Ex-: Bill system, payroll system, Stock control system.

Management information systems (MIS)

- This is the second category of information systems, consisting of hardware and software integration allowing the organization to perform its core functions.
- They help in obtaining data from various online systems.
- The data thus obtained is not stored by the system; rather, it is analyzed in a productive manner to help in the management of an organization.
- The purpose of a management information system is to transform comparatively raw data accessible through using Transaction Processing System into a summarized and aggregated form for managers, generally in the form of a report.
- Operational supervisors and middle management are likely to use the reports.

Decision support systems (DSS)

- Decision support system. It is interactive, which offers information, data manipulation tools, and models to support decision-making in a semi-structured and unstructured scenario.
- This type of information system includes tools and techniques to help gather relevant information and examine options, and substitutes, the end-user being more elaborate in making DSS than MIS.
- An organization can make an informed decision about its operations using decision support systems.
- It analyses the rapidly changing information that cannot be determined in advance.
- It can be used in completely automated systems and human-operated systems.

However, for maximum efficiency combination of human and computer-operated systems is recommended.

Experts information System (EIS)

- The expert system contains expertise which is helpful for a manager in identifying problems or in problem-solving.
- The principles of artificial intelligence research are used to develop these kinds of information systems.
- This type of information system is a knowledge-based system.
- It acts as an expert consultant to users by utilizing its knowledge of a specific area.
- There are some components of expert systems such as Knowledgebase and software modules.



Information Security

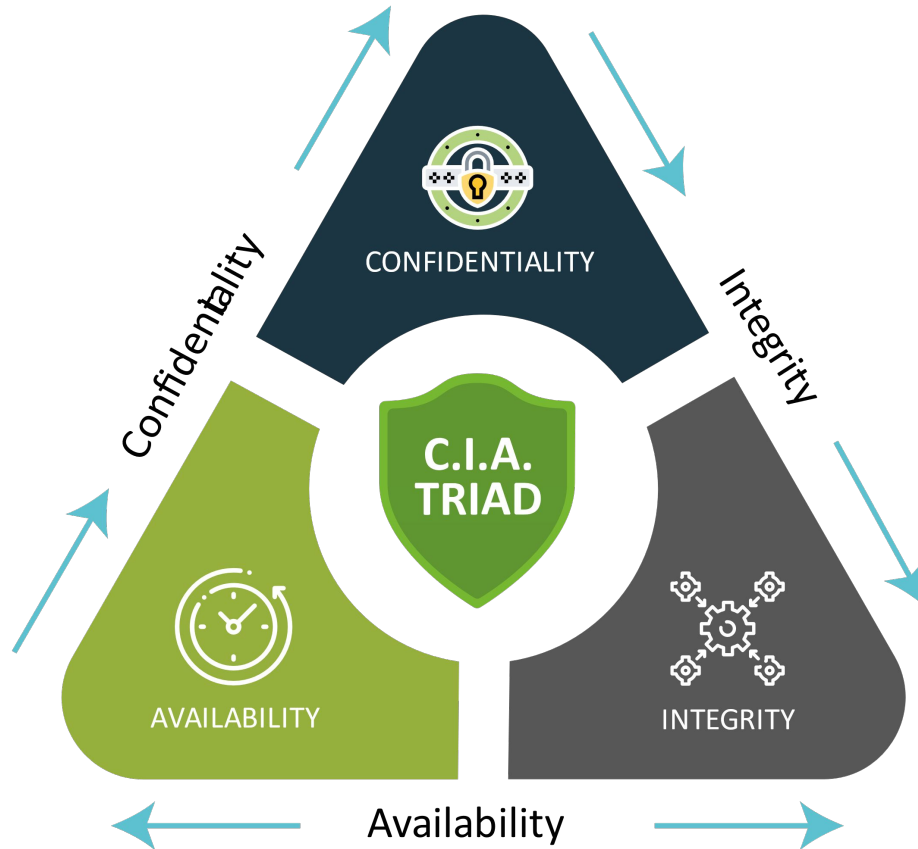


Information Security

- Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- Information can be physical or electronic one.
- Information security is designed and carried out to protect the print, digital, and other private, sensitive, and private data from unauthorized persons.
- Information Security programs are build around 3 objectives, commonly known as CIA



CIA – Confidentiality, Integrity, Availability



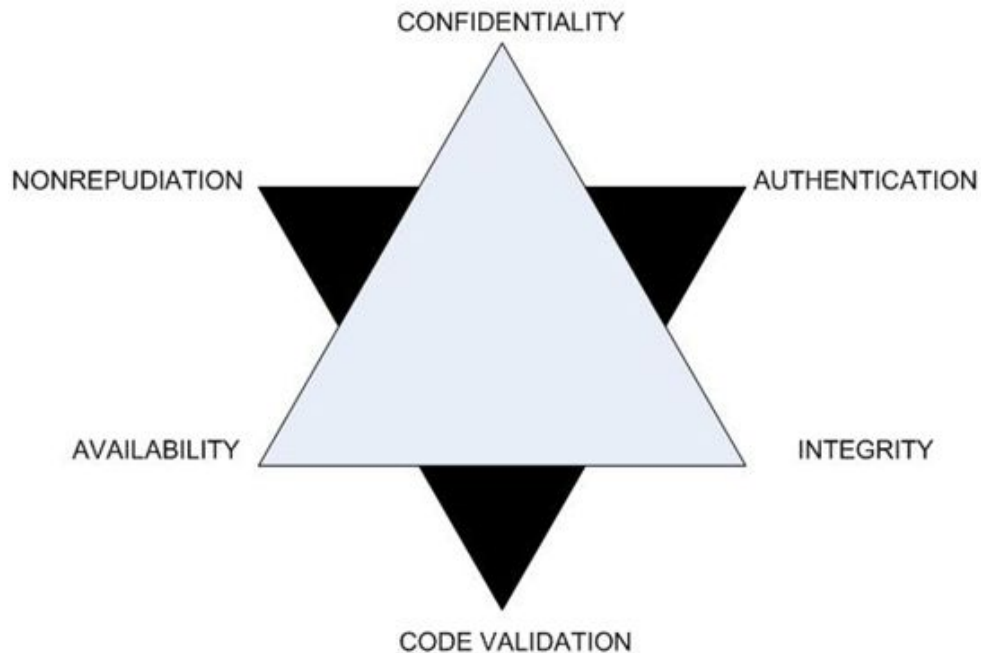
CIA

- The CIA triad is a model designed to guide policies for the information security of an organization.
- It combines the three principles that should form the security infrastructure of any organization:

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability

- This are...

- ☐ Non repudiation
- ☐ Authenticity
- ☐ Accountability



Confidentiality

- Confidentiality is the first pillar of the CIA TRIAD and is concerned with controlling access to critical data and preventing any unauthorized disclosure of it.

OR

- Confidentiality is the process of keeping an organization or individual's data private and ensuring only authorized people can access it.



Integrity

- Integrity Means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.
- In cybersecurity, integrity refers to data that hasn't been tampered with. Data that has been tampered with or compromised has lost its integrity.



Availability

- Availability means information must be available when needed.
- Authorization ensures that the certain users can get timely and reliable access to the required resources whenever they need to.



Non repudiation

- Non repudiation means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction.
- Data Integrity and Authenticity are pre-requisites for Non repudiation.

Authenticity

- Authenticity means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.
- This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission.

Accountability

- Means that it should be possible to trace actions of an entity uniquely to that entity.

How Might CIA Be Breached?

- Eavesdropping attacks.
- Encryption cracking.
- Malicious insiders.
- Man-in-the-middle attack



Need for Information Security

1. Protecting the functionality of the organization
2. Enabling the safe operation of applications
3. Protecting the data that the organization collect and use
4. Safeguarding technology assets in organizations



Threats to Information Systems

- In Information security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a Devices
- A threat is a statement indicating that you will cause harm to or create some other kind of negative consequences for someone.
- Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization

Software attacks means attack by Viruses, Worms, Trojan Horses etc.

Malware is a combination of 2 terms- Malicious and Software.

- So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system.

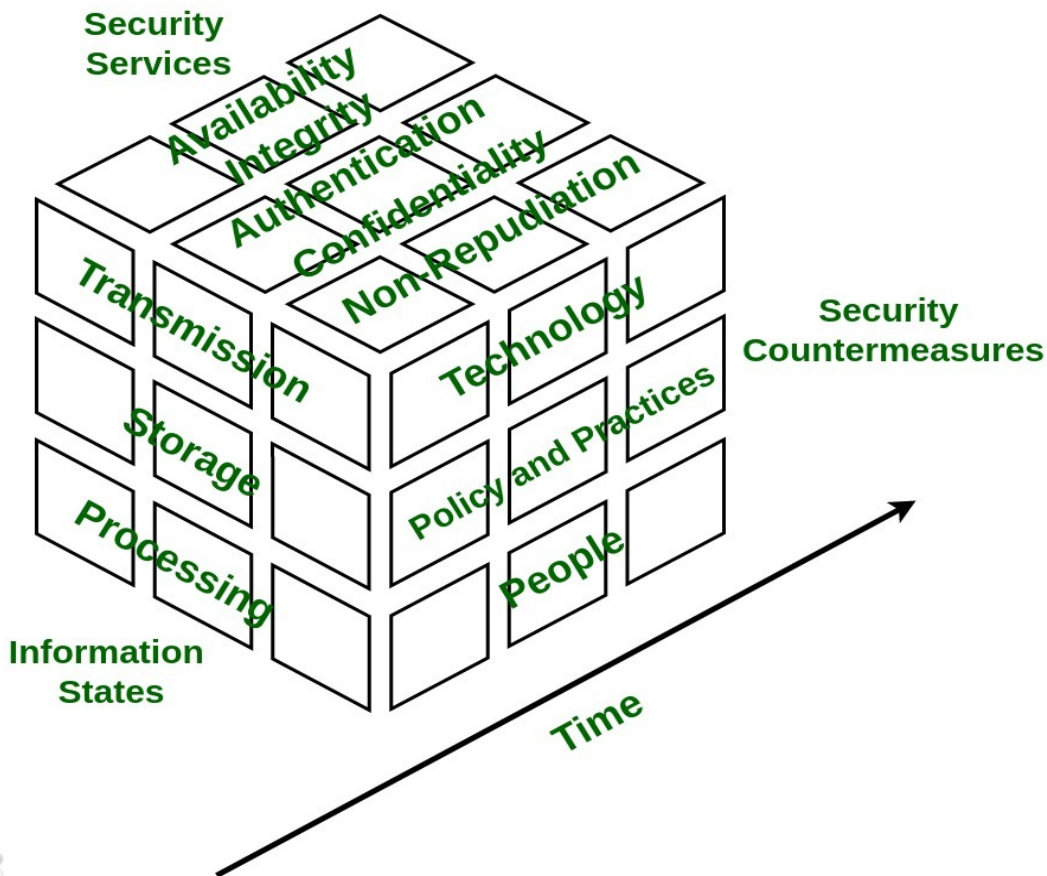
Information Assurance

- Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
- It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

Information Assurance Model

1. Information States
2. Security Services
3. Security Countermeasures
4. Time

Information Assurance Model



1) Information States

- Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

2) Security Services

- It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

3) Security Countermeasures

- This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

4) Time

- This dimension can be viewed in many ways.
- At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access.

Cyber Security and Security Risk Analysis

- A security risk assessment identifies, assesses, and implements key security controls in applications.
- Risk analysis defines the review of risks related to the specific action or event.
- The risk analysis is used to information technology, projects, security issues and some other event where risks can be analyzed based on a quantitative and qualitative basis.

Risk Analysis

Process



Risk Identification:

- Risk identification involves brainstorming activities.
- It also involves the preparation of a risk list.
- Brainstorming is a group discussion technique where all the stakeholders meet together.
- This technique produces new ideas and promotes creative thinking.
- Preparation of risk list involves identification of risks that are occurring continuously in previous software projects.

Risk Analysis and Prioritization:

- Identifying the problems causing risk in projects
Identifying the probability of occurrence of problem
- Identifying the impact of problem
- Assigning values to step 2 and step 3 in the range of 1 to 10
- Calculate the risk exposure factor which is the product of values of step 2 and step 3
- Prepare a table consisting of all the values and order risk on the basis of risk exposure factor

Risk Avoidance and Mitigation:

- The purpose of this technique is to altogether eliminate the occurrence of risks.
- So the method to avoid risks is to reduce the scope of projects by removing non-essential requirements.



Risk Monitoring:

- In this technique, the risk is monitored continuously by reevaluating the risks, the impact of risk, and the probability of occurrence of the risk.
- This ensures that:
 - Risk has been reduced
 - New risks are discovered
 - Impact and magnitude of risk are measured



Thanks!

Any questions?

You can find me at:

@Abhidave87427142 & abhijit@techdefence.com

@Abhijit-dave

