# UNIT-I

## Information System

**An information system (IS)** is a set of components that interact to collect, process, store, and distribute information to support decision-making, coordination, control, analysis, and visualization in an organization. There are several types of information systems, each with specific functions and uses within an organization.

An information system has **five core components**:

- **Hardware:** Physical components like computers, smartphones, and network equipment.
- **Software:** The programs and applications that process data.
- **Data:** Raw information that is collected and stored, often in a database.
- **Networks:** Communication systems that connect different components and allow for data sharing.
- **People:** The users, managers, and developers who interact with and use the system.

**Types of Information Systems:**

1. Transaction Processing Systems (TPS):

These systems handle day-to-day routine transactions, such as sales orders, payroll, and inventory updates. They are the foundation for many other systems, providing the raw data for analysis and reporting.

2. Management Information Systems (MIS):

MIS systems provide summarized reports and information to middle managers to help them monitor and control the organization's performance. They often rely on data from TPS to generate these reports.

3. Decision Support Systems (DSS):

DSS systems are interactive tools that help managers make decisions, especially for semi-structured or unstructured problems. They provide analytical and modeling capabilities to evaluate different scenarios.

4. Executive Information Systems (EIS):

EIS systems provide senior executives with a broad overview of the organization's performance, often through highly summarized reports and dashboards. They are designed to support strategic decision-making.

5. Knowledge Management Systems (KMS):

KMS systems focus on capturing, storing, and sharing knowledge and expertise within an organization. They help employees access and utilize valuable information for problem-solving and innovation.

6. Enterprise Resource Planning (ERP) Systems:

ERP systems integrate all aspects of a business, including finance, human resources, supply chain management, and customer relationship management, into a single, unified system.

7. Office Automation Systems (OAS):

OAS systems automate routine office tasks, such as word processing, email, and scheduling, to improve efficiency and productivity.

8. Expert Systems (ES):

Expert systems are designed to mimic the decision-making abilities of a human expert in a specific domain. They use knowledge bases and inference rules to provide advice and solutions to complex problems.

9. Business Intelligence Systems (BIS):

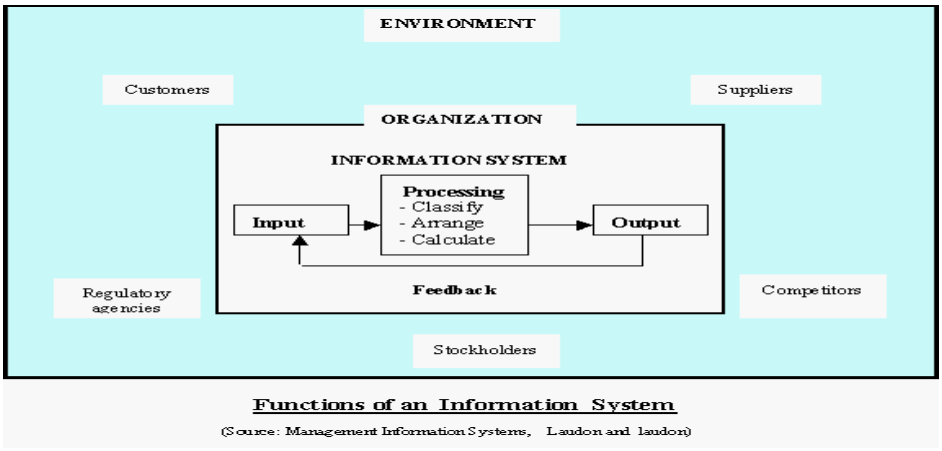
BIS systems analyze large amounts of data to identify trends, patterns, and insights that can be used to improve business performance. They often incorporate data mining,OLAP, and reporting tools.

10. Customer Relationship Management (CRM) Systems:

CRM systems manage all aspects of a company's interactions with its customers, including sales, marketing, and customer service.

**Purpose of Information Systems: -**

- **Support Decision**-Making: Help managers analyze data and make informed decisions.
- **Enhance Business Processes:** Streamline operations and improve efficiency.
- **Facilitate Communication:** Provide platforms for gathering and distributing information.
- **Solve Complex Problems:** Offer solutions in specialized areas like medicine (e.g., expert systems).




Functions of an Information System

(Source: Management Information Systems, Laudon and laudon)

**Fig: - Functions of an IS**

**Development of Information System: -**

The development of an information system follows a lifecycle, with the Software/System Development Life Cycle (SDLC) being a common framework.

1. **Planning:** Recognizing the problem and defining the project's scope and goals.
2. **Analysis:** Gathering facts, understanding the existing system, and specifying the requirements for the new system.
3. **Design:** Detailing how the new system will function to meet the identified requirements.
4. **Construction/Development:** Building and coding the system.
5. **Implementation:** Installing and deploying the new system.
6. **Testing:** Evaluating the system to ensure it functions correctly.
7. **Maintenance and Review:** Ongoing updates, bug fixes, and improvements to keep the system effective over time.

This iterative process helps ensure that the final information system is of high quality and meets the user's needs in terms of time, cost, and effectiveness.

## Information security

**Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Many businesses are solely based on information stored in computers. Personal staff details, client lists, salaries, bank account details, marketing and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate.

Information security systems need to be implemented to protect this information. Effective information security systems incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners are not enough on their own to protect information. A set of procedures and systems needs to be applied to effectively deter access to information.

### Principal of information security

1. Confidentiality
2. Integrity and
3. Availability

### Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

### Integrity

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases. Integrity is violated when a message is

actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

**Availability**

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

## Need for Information security

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

## Information System Threats

A threat is anything (man made or act of nature) that has the potential to cause of harm. A threat is also defined as "A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability".

Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. In this context, a threat is a potential or actual adverse event that may be malicious (such as denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise.

## Classification of Security Threats

In order for one to produce a secure system, it is important to classify threats. The classification

of threats could be:

1. Physical threats, 2. Accidental error,

3. Unauthorized access, 4. Malicious misuse.

**Physical Threat**

Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

Another good example of a physical threat to computer system is the flooding of the city of New Orleans (Hurricane Katrina) during which valuable information was lost and billions of computer data were destroyed.

**Accidental Error**

This is also an important security issue which computer security experts should always put into consideration when designing security measures for a system. Accidental errors could occur at any time in a computer system but having proper checks in place should be the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator errors.

**Unauthorized access**

Data stored on the computer system has to be accessed for it to be translated into useful information. This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media. Considering an example of an organization in which a member of staff at a particular level of hierarchy within the establishment is only allowed access to specific area according to the policy of the organization. If these employees by other means not set in the organization policy gain access to the restricted data area on the computer, this can be termed an unauthorized access.

**Malicious misuse:**

Any form of tampering of the computer system which includes penetration, Trojan horses' viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases.

## Information system attacks

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Attacks are classified in two categories such as:

1. Passive attacks

2. Active 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. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. These protections apply to data in transit, both physical and electronic forms as

well as data at rest in various types of physical and electronic storage facilities. Information assurance as a field has grown from the practice of information security.

Information Assurance (IA) is the process of getting the right information to the right people at the right time. IA adds business benefit through the use of Information Risk Management, Trust Management, Resilience, appropriate Architecture, system safety, and security, which increases the utility of information to authorized users and reduces the utility of information to those unauthorized. It is strongly related to the field of information security, and also with business continuity. IA relates more to the business level and strategic risk management of information and related systems, rather than the creation and application of security controls. Therefore, in addition to defending against malicious hackers and code (e.g., viruses), IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems. Further, while information security draws primarily from computer science, IA is an interdisciplinary field requiring expertise in business, accounting, user experience, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to computer science. Therefore, IA is best thought of as a superset of information security (i.e. umbrella term), and as the business outcome of Information Risk Management.

## Security Risk Analysis

Many organizations suffer "security paralysis," a condition in which it is impossible to prioritize areas for remediation due to limited resources.

For many organizations, the best approach may be to pursue an internal cyber-security risk assessment. There are few following step plan to help organizations lay the foundation for a meaningful security strategy.

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

# Cyber Security

Cyber security is the practice of protecting networks, devices, programs, and data from digital attacks and unauthorized access to ensure confidentiality, integrity, and availability of information. It involves technologies, processes, and people to defend against threats like malware, phishing, and ransomware, and includes areas such as network security, application security, and data security. Effective cybersecurity relies on strong security measures, regular software updates, strong passwords, and user awareness to safeguard digital systems.

Key Concepts

- Confidentiality: Ensuring that sensitive information is only accessible to authorized individuals.
- Integrity: Protecting data from unauthorized modification or deletion.
- **Availability:** Ensuring that systems and data are accessible and operational when needed.

Types of Cyber security

- Network Security: Protecting computer networks from intrusions and unauthorized access.
- Application Security: Securing software and devices to prevent threats within applications.
- Information Security: Protecting the privacy and integrity of data, whether stored or being transmitted.
- Operational Security: Managing processes and decisions to handle and protect data assets.
- Disaster Recovery & Business Continuity: Planning for how an organization will respond to a cyberattack or other incident causing data or operational loss.

Common Cyber Threats

- Malware:

Malicious software designed to harm or gain unauthorized access to computer systems.

- Phishing:

Attempts to trick individuals into revealing sensitive information or downloading malware through deceptive emails or messages.

- Ransomware:

A type of malware that encrypts a victim's files and demands a ransom payment to restore access.