8/19/2022

UNIT - I

INFORMATION SYSTEM

by

Mr. Ajay Kumar Badhan

Assistant Professor

M.TECH[CST], B.TECH [CSE]

Email: ajay.27337@lpu.co.in

Personal Blog: https://ajaykumarbadhan.wordpress.com/

Preferred Text Book

- Information System Security Wiley Publications by Nina Godole, Wiley
- Computer Security: The Complete Reference Roberta: Tata Mcgraw Gill by Bragg, Mcgraw Hill Edition

CONTENT

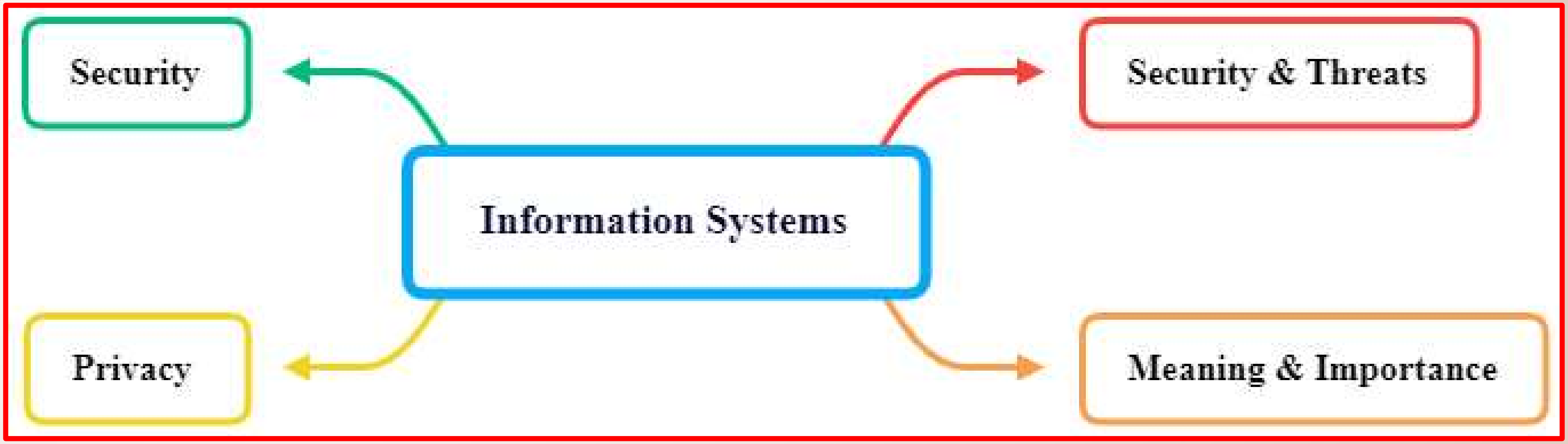
INFORMATION SECURITY

- Information Security & Threats
- Meaning of Information System
- Importance of information System
- Information Security
- Privacy Threat

BUILDING BLOCKS

- Principles
- Terms
- Three Pillar of Information Security
- Risk Management
- Risk Analysis
- Information Classification
- Approaches and Considerations

CONTENT - GRAPHICAL PRESENTATION



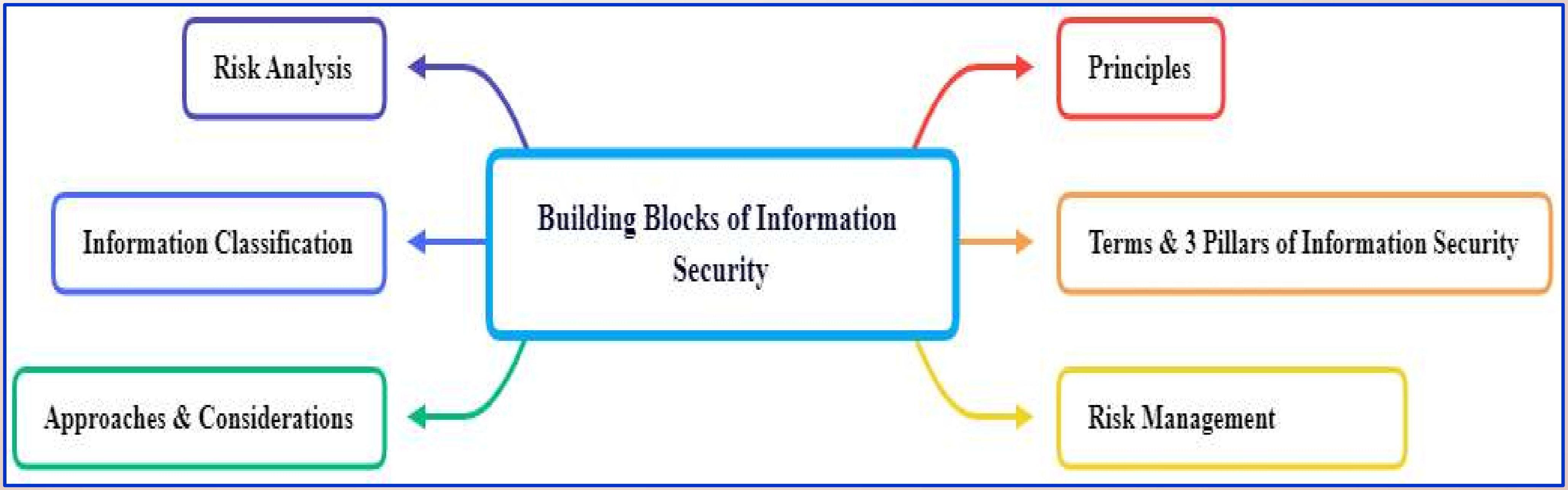
Information Systems

Security

Privacy

Security & Threats

Meaning & Importance



Building Blocks of Information Security

Risk Analysis

Information Classification

Approaches & Considerations

Principles

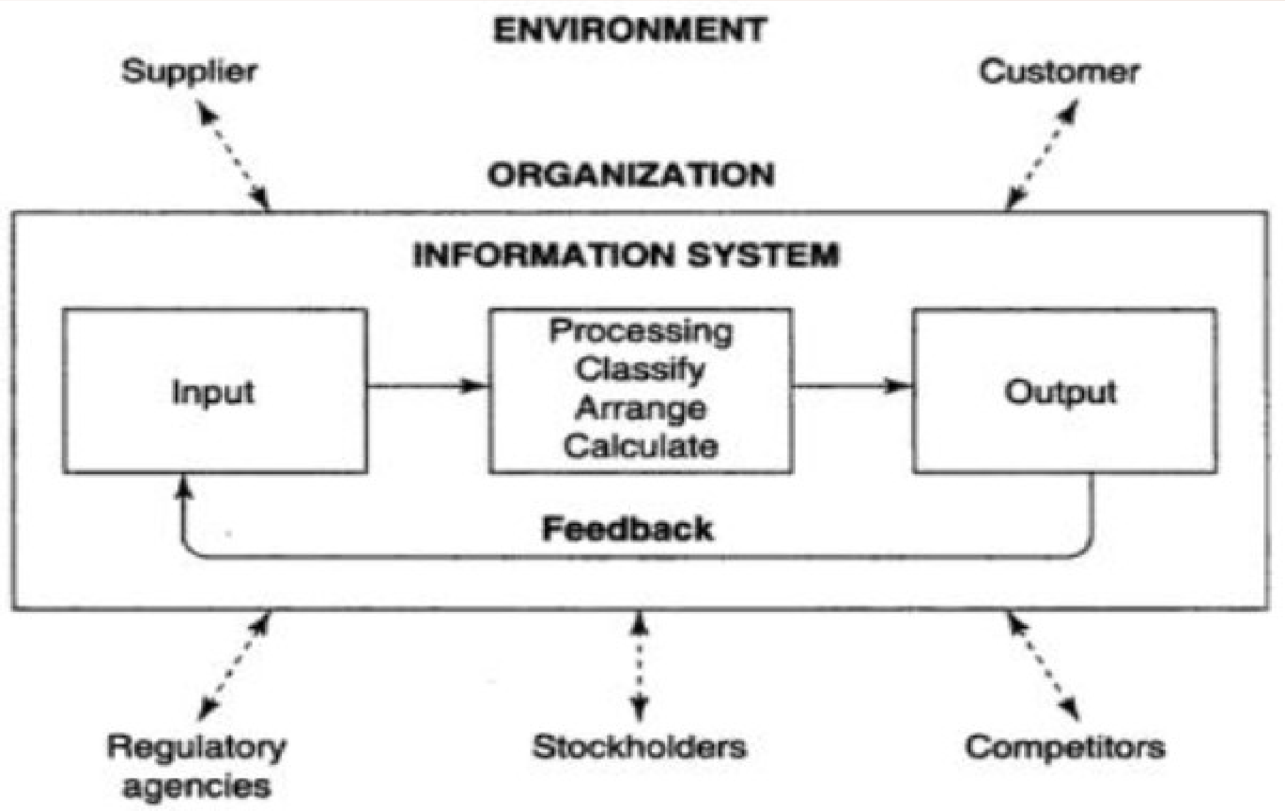
Terms & 3 Pillars of Information Security

Risk Management

INTRODUCTION – INFORMATION SYSTEM

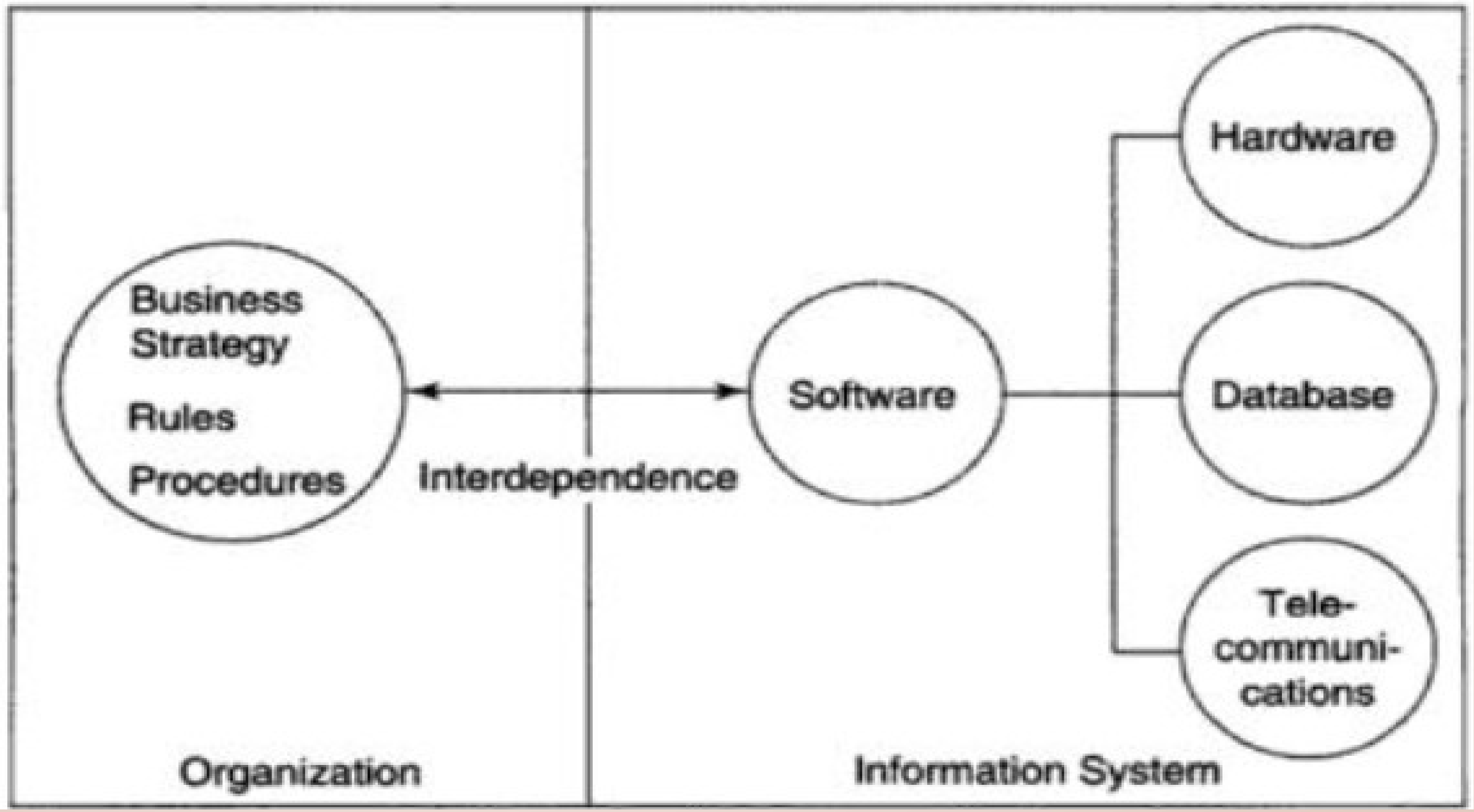
Basic Introduction

1. An Information system is a group of components that interact to produce information
2. It is an **integrated** and **cooperating** set of **software-directed information technologies** supporting individual, group, organizational, or societal goals.
3. It is the study of complementary networks that people and organizations use to collect, filter, process, create, and distribute data.



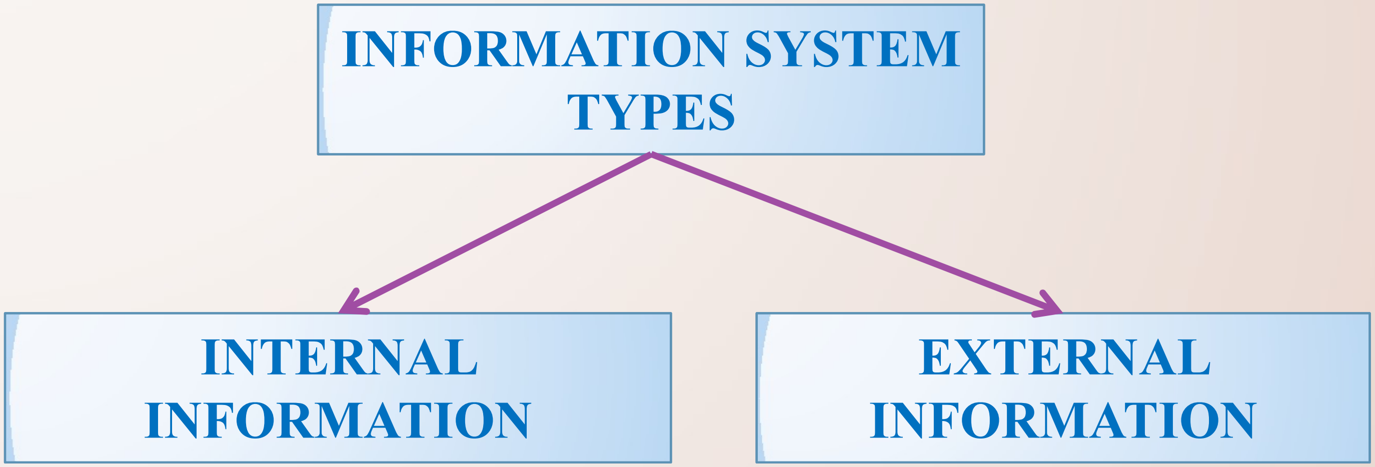
INTRODUCTION – INFORMATION SYSTEM

Functions of Information System



INFORMATION SYSTEM - TYPES

Information System

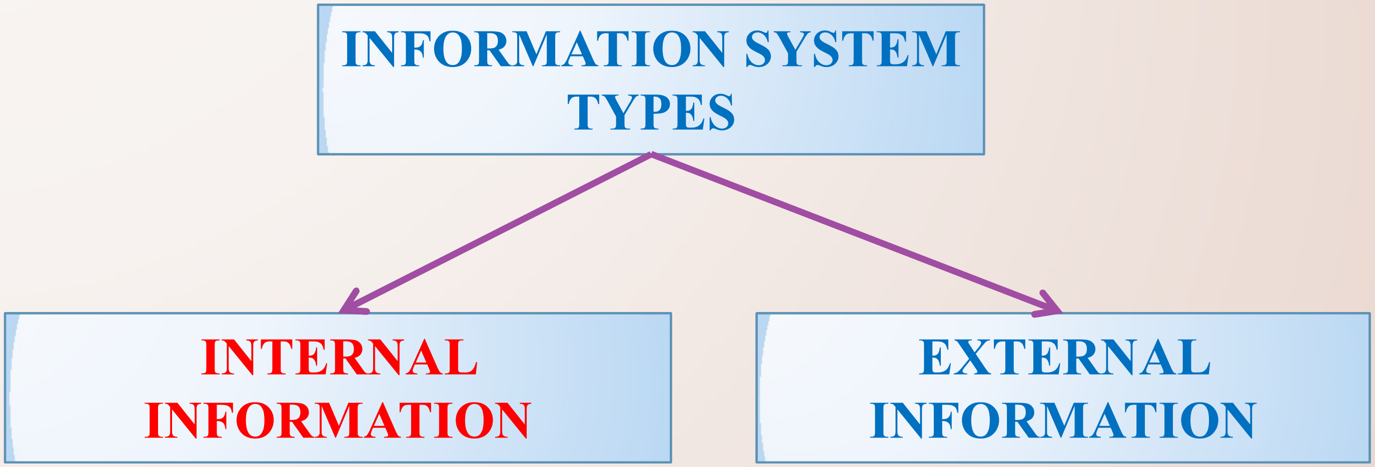

INFORMATION SYSTEM TYPES

INTERNAL INFORMATION

EXTERNAL INFORMATION

INFORMATION SYSTEM - TYPES

Information System



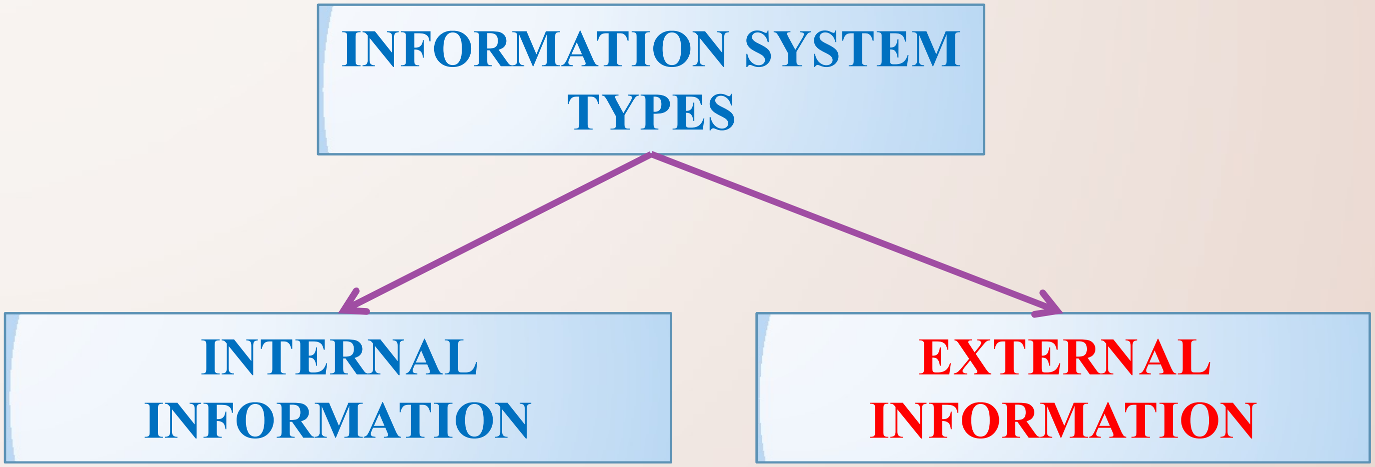
INTERNAL INFORMATION

1. The information which is collected from the **sources**, **internal to the organization** is called Internal Information.
2. This information is generated from the operations of the organization at the various **functional levels**
3. They always pertain to the various operational units of the organization.
4. The internal information is generally required by the **middle** or **supervisory level of management**

Examples: Production figures, **sales forecast**, **budgets**, **stock level**, **employee data**, **accounting reports**

INFORMATION SYSTEM - TYPES

Information System



EXTERNAL INFORMATION

1. The information which is collected from the sources **external to the organization** is called External Information.
2. These are generated in the **external environment** of the organization
3. They are considered to **affect** the organizational performance in the external environment
4. It is generally required by **top-level management**.
5. It is used in the **planning process of management** to give the shape of its future.

Examples: Govt. Policies, **Economic Trends**, **Market Information**, **Competitive Information** etc

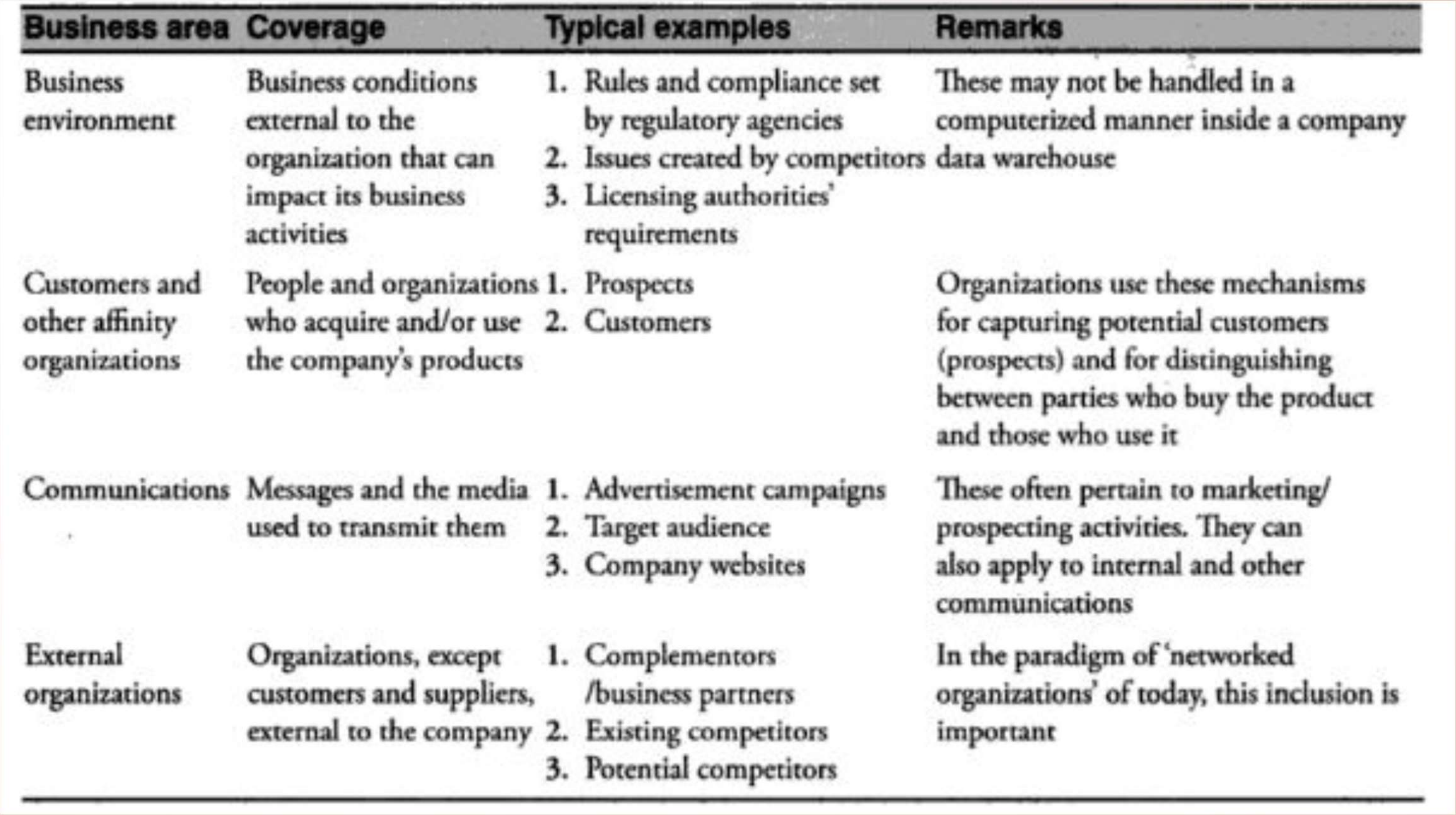
INFORMATION SYSTEM - INTRODUCTION

Information System Roles & It’s Management

1. It helps managers in effective **decision-making**
2. Based on IS, organization will gain edge in the competitive environment.
3. IS helps taking **right decision** at the right time.
4. Knowledge gathered through Information System is useful in unusual situation.
5. It can be integrated to formulate a strategy of action.
6. It ensures **pervasiveness** of decision making.
7. It makes the organization transparent
8. It helps managerial learning about organization.

INFORMATION SYSTEM - INTRODUCTION

Business Area Wise Organization of Information

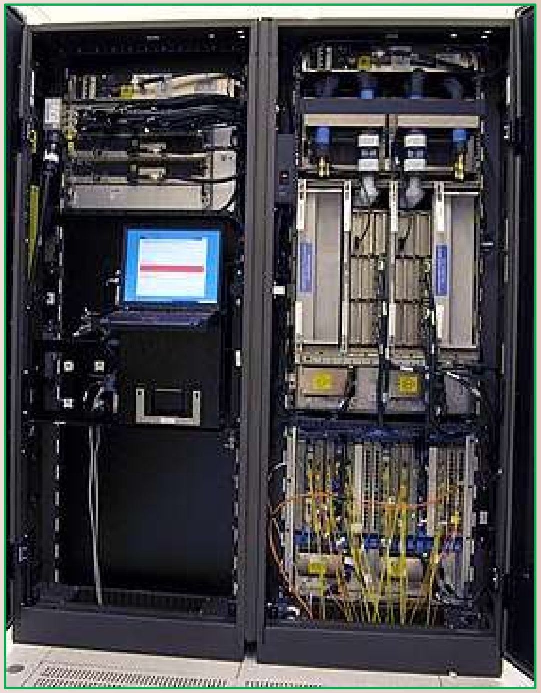


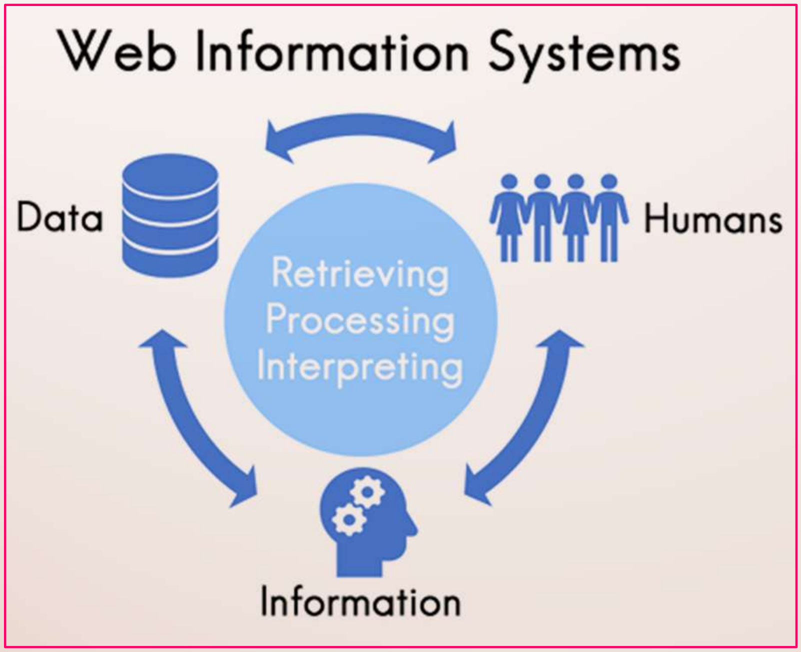
Business area	Coverage	Typical examples	Remarks
Business environment	Business conditions external to the organization that can impact its business activities	1. Rules and compliance set by regulatory agencies 2. Issues created by competitors 3. Licensing authorities' requirements	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company's products	1. Prospects 2. Customers	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	1. Advertisement campaigns 2. Target audience 3. Company websites	These often pertain to marketing/ prospecting activities. They can also apply to internal and other communications
External organizations	Organizations, except customers and suppliers, external to the company	1. Complementors /business partners 2. Existing competitors 3. Potential competitors	In the paradigm of 'networked organizations' of today, this inclusion is important

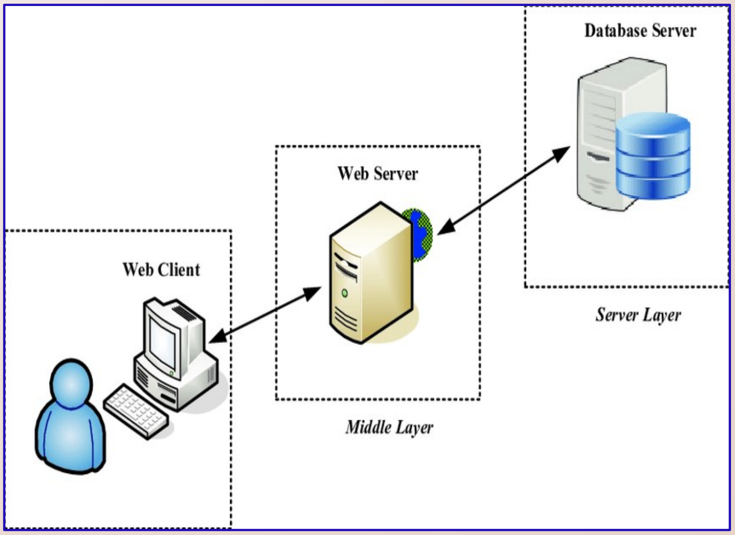
INFORMATION SYSTEM - INTRODUCTION

Changing Nature of Information System

1. Maine Frame Based Information System
2. Client-Server based Information System
3. Web-based Information System







INFORMATION SYSTEM – Security & Threat

Mis-use of Information systems leads to:

1. **Loss of Productivity**
2. **Loss of Revenue**
3. **Legal Liabilities**
4. **Work Place issues**

PILLARS OF INFORMATION SECURITY

The CIA triad refers to an information security model made up of the three main components:

1. **Confidentiality,**
2. **Integrity and**
3. **Availability**

CONFIDENTIALITY

1. It is used to prevent the **intentional** or **unintentional** unauthorized disclosure of message content
2. It can occur in many ways, such as through the intentional release of **private information of a company** or **through a misapplication of network rights**.
3. Confidentiality is concerned with **preventing** the unauthorized disclosure of sensitive information
4. It is associated with **secrecy** and the use of **encryption.** It means the data is only available for authorized parties.

Example: Bank never gives information about a client to another person.

Some more examples:

1. Suppose there a computer in which there is some important data is saved. Confidentiality means there should be a trust that data will be accessed by you or a dedicated user only. Access to that data will be only through an authorized person.

PILLARS OF INFORMATION SECURITY

The Three Pillars of Information Security are:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

INTEGRITY

1. It refers to the certainty that the data is **not tampered** with or degraded during or after submission.
2. It means no one can modify or later contents of information other than the owner.
3. Prevention of the modification of information by unauthorized users.

   Example: Suppose user-1 sends a message **"Hi"** to user-2. The message sent should not be modified in between

3. Preservation of the **internal** and **external** consistency
4. Internal consistency ensures that data is consistent.

Examples:

1. Only authorized users can change the password of their Facebook account. Internally data should be maintained
2. No one can do transactions from a user account except the user itself.

PILLARS OF INFORMATION SECURITY

The Three Pillars of Information Security are:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

AVAILABILITY

1. It assures that a **system's authorized** users have timely and uninterrupted access to information in the system and to the network.
2. It means that the **information** is available to the authorized user when it is needed.
3. For a system to demonstrate availability, it must have properly **functioning computing systems**, **security controls**, and **communication channels**.
4. Systems defined as **critical** often have extreme requirements related to availability.

Example: The user wants to access the FB account during midnight, the server should be available to serve it

INFORMATION SECURITY - TERMS

Important Terms

1. Identification **2. Authentication** **3. Accountability** **4. Authorization**

IDENTIFICATION

1. It indicates the means by which users claim their identities to a system. It is most commonly used for **access control** and is necessary for **authentication** and **authorization**.
2. It is the ability to identify uniquely a user of the system or an application that is running in the system

Examples: Login ID, Identity Card of employees in any organization

AUTHENTICATION

1. It is the **testing** or **reconciliation** of evidence of the user's ID. It establishes a user's ID and ensures that the user is who they say they are.
2. It is the ability to prove that a user or application is genuinely who or what the application claims to be.
3. It is a **security measure** designed to establish the **validity of a transmission**, **message**, or **originator** or a means of verifying an individual's eligibility to receive specific categories of information

INFORMATION SECURITY - TERMS

Important Terms

1. **Identification** 2. **Authentication** 3. **Accountability** 4. **Authorization**

ACCOUNTABILITY

1. A system's ability to determine the actions and behavior of a single individual within a system and to identify that particular individual. Audit trails and los support accountability

Examples:

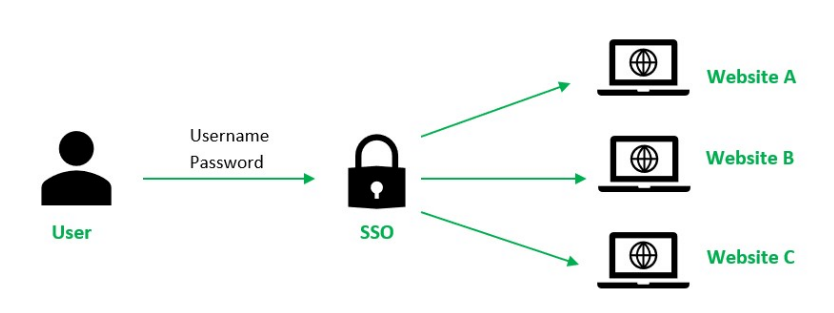
AUTHORIZATION

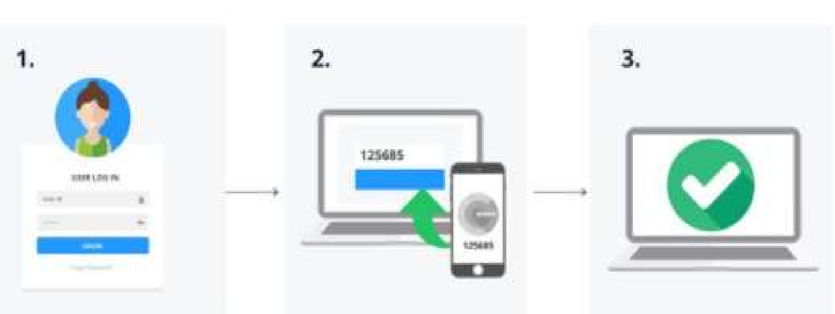
1. The rights and permissions granted to an individual (or process), which enables access to a computer resource.
2. Once the user identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold. It is the access rights granted to the user, program, or process.
3. It protects critical resources in a system by limiting access to the resources to authorized users and their applications. It prevents the unauthorized use of resources.

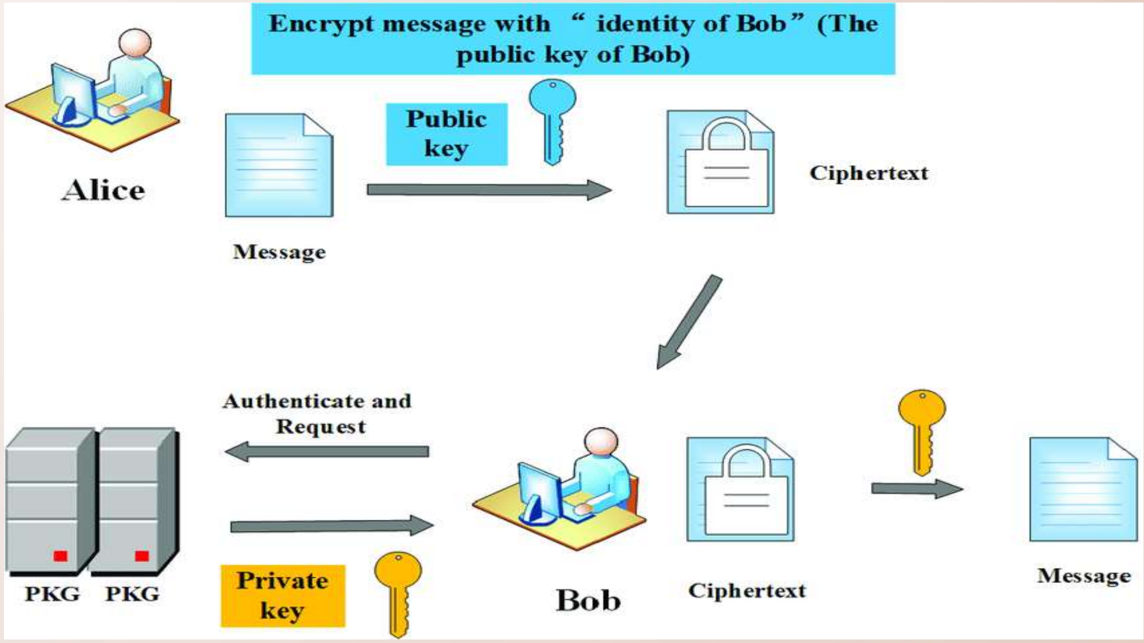
INFORMATION SECURITY - TERMS

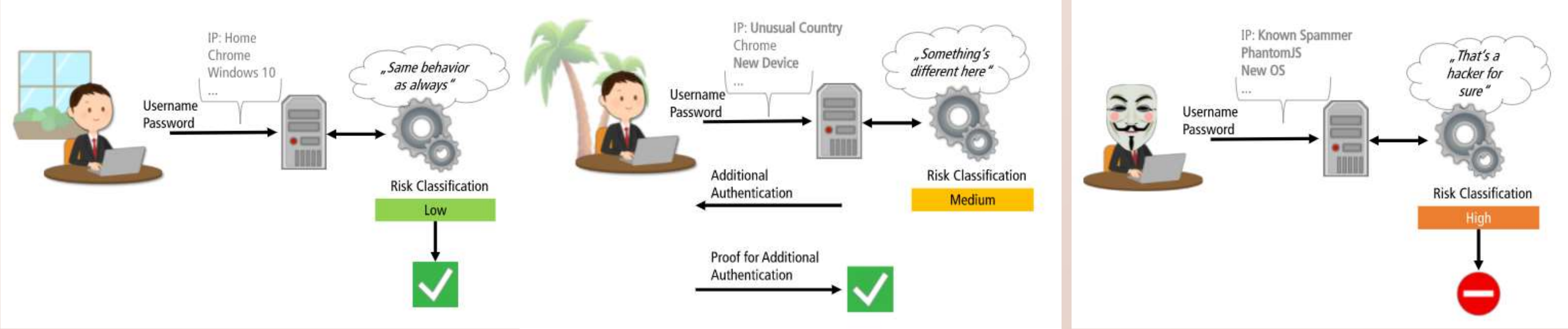
Important Terms

1. Identification
2. Authentication
3. Accountability
4. Authorization





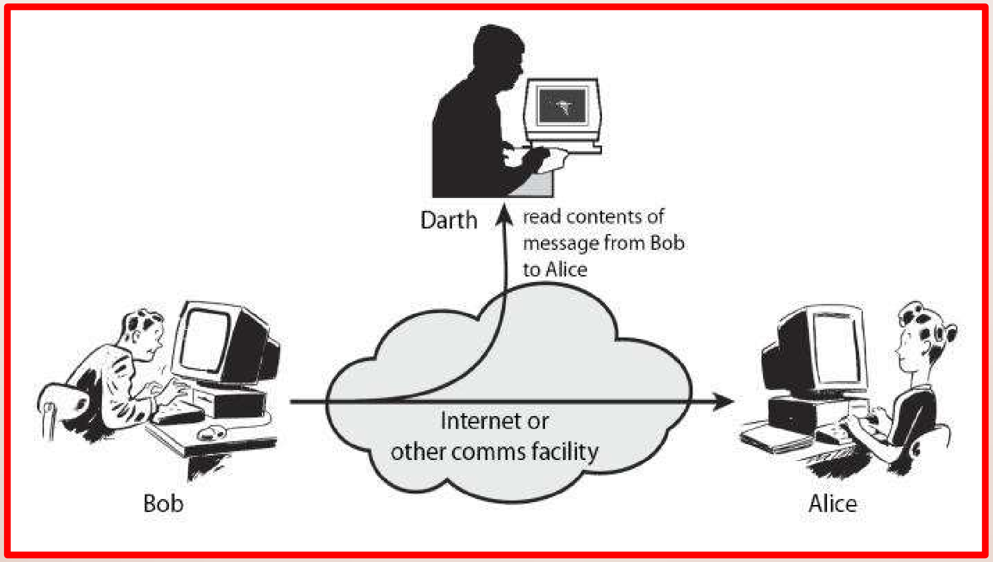


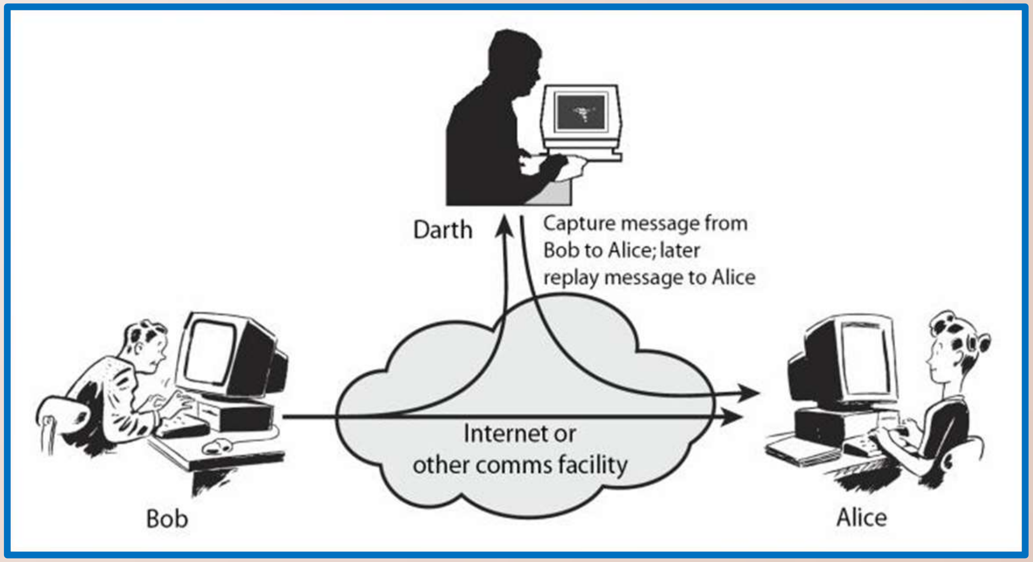


INFORMATION SECURITY - ATTACKS

Security Attacks

1. Any action that compromises the security of information owned by another organization
2. Information Security is about how to prevent attacks or falling, to detect attacks on information-based systems
3. Have a wide range of attacks:
   1. **Passive Attack** ⇒ In this the attacker observes the messages and copies them
   2. **Active Attack** ⇒ In this, the attacker tries to modify the content of the messages.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

INFORMATION SECURITY - ATTACKS

Basic Terms in Security Attacks:

There are 3 terms:

1. **Threat** ⇒ It is an object, person, or other entity that represents a constant danger to an asset.
2. **Vulnerability** ⇒ A weakness that allows an attacker to reduce the systems information assurance.

   At the intersection of **3** elements:

   a. **system susceptibility of the flaw**,

   b. **attacker access to the flaw**,

   c. **attacker capability to exploit the flaw.**

3. **Countermeasures** ⇒ The measures that are implemented to overcome the threats and vulnerabilities.

   Examples: Cryptography, Ciphertext, Cesare Cipher etc.

INFORMATION SECURITY - ATTACKS

Information Level Threats

1. Spreading wrong information ex- hoaxes
2. Involves purposeful dissemination of information
3. Sending fake inquiries
4. Setting up revenge websites
5. Falsifies Job advertisements

Network-Based Threats

1. **Hacking of Computer System**

2. Denial of Service

DOS

1. Flooding accounts with a large number of emails is a network-based attack as it is the size and the quantity of the email that matters and not the content of the email.
2. Before the rise of the internet attacks were physical but nowadays attacks are through networks.

Example: Amazon Web Services (AWS) reports that in February 2020, they defended against a **2.3 - terabit-per-second (Tbps) distributed denial of service (DDoS) attack!**

INFORMATION SECURITY - PRINCIPLES

Principle Source of Security Threats

1. **Human Error:**

   When an employee discloses confidential information it comes under human error.

2. **Computer Abuse or Crime:**

   When a person intends to be malicious ex fake rumors like you have won a lottery

3. **Natural Disasters:**

   This can happen in the form of natural calamities, wars, and riots.

4. **Failure of Hardware and Software:**

   Server malfunctioning and software errors

INFORMATION SECURITY - PRINCIPLES

Security Threats Related to Computer Abuse or Crime

1. **Impersonation:**

   The impersonator enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.

2. **Trojan Horse**

   Concealing within an authorized program a set of instructions that will cause unauthorized actions.

3. **Logic Bombs:**

   unauthorized actions are often introduced with the Trojan horse technique, which stays dormant until a specific time comes, as the instruction may keep checking the system's internal clock.

4. **Computer Virus:**

   A segment of code that is able to perform malicious acts and insert copies of themselves into other programs in the system. Because of this replication, a virus will progressively infect healthy programs and systems.

INFORMATION SECURITY - PRINCIPLES

Security Threats Related to Computer Abuse or Crime

5. **Denial of Service (DOS):**

   - Rendering the system unusable by legitimate users.

6. **Dial Diddling**

   - Changing data before or during input, often to change the contents of a database.

7. **Salami Technique:**

   - It's a type of cybercrime in which an attacker steals money in small amounts.
   - **Two variants:** Salami Slicing, and Penny Shaving

8. **Spoofing:**

   Configuring a system to masquerade as another system on the network in order to gain unauthorized success.

9. **Super-Zapping:**

   Using a system's program that can bypass regular system controls to perform unauthorized acts.

10. **Scavenging**

   Unauthorized access to information by searching through the residue after a job has been run on a computer. E.g. printer.

INFORMATION SECURITY - PRINCIPLES

Security Threats Related to Computer Abuse or Crime

11. Data Leakage

- The unauthorized transmission of data from an organization to any external resource.
- The data can be leaked physically or electronically via hard drives, USB devices, mobile phones, etc., and could be exposed publicly or fall into the hands of a cyber-criminal.

12. Wire Tapping

Tapping computer TC lines to obtain information

INFORMATION SECURITY - TERMS

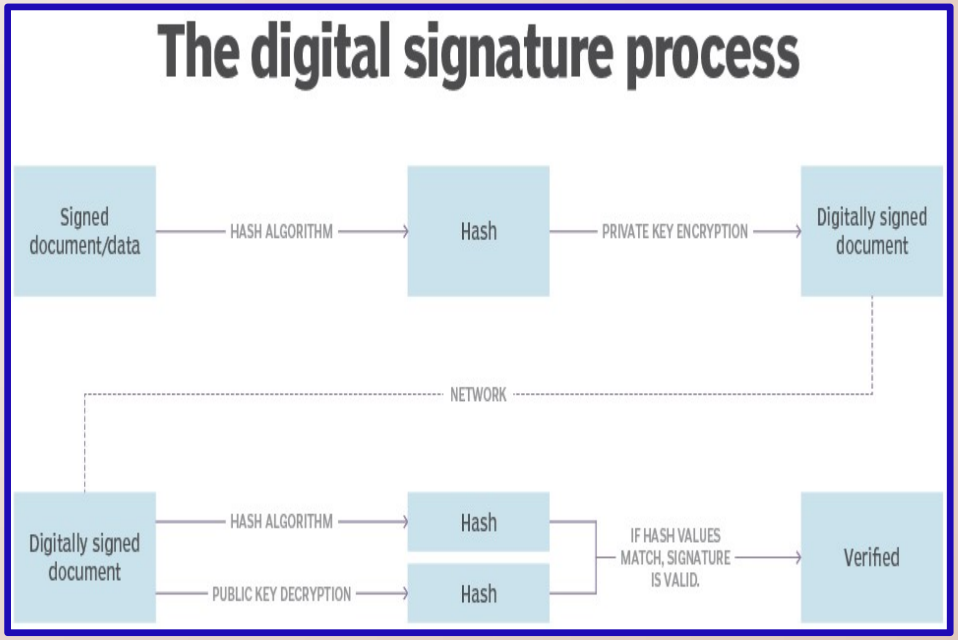
TERMS & DEFINITION

1. Non-Repudiation

- Assurance that someone cannot deny the validity of something.
- It prevents either the sender or receiver from denying a transmitted message.
- Crucial to E-Commerce
- Without it an individual or entity can deny that he/she is not responsible for a transaction, therefore not financially liable.

2. Electronic or Digital Signature

- A digital code generated by a public key encryption
- The appended data or a cryptographic transformation applied to any data unit allows to prove the source and integrity of the data unit and protects against forgery.


The digital signature process
Signed document/data
HASH ALGORITHM
Hash
PRIVATE KEY ENCRYPTION
Digitally signed document
NETWORK
Digitally signed document
HASH ALGORITHM
Hash
PUBLIC KEY DECRYPTION
Hash
IF HASH VALUES MATCH, SIGNATURE IS VALID.
Verified

INFORMATION SECURITY - TERMS

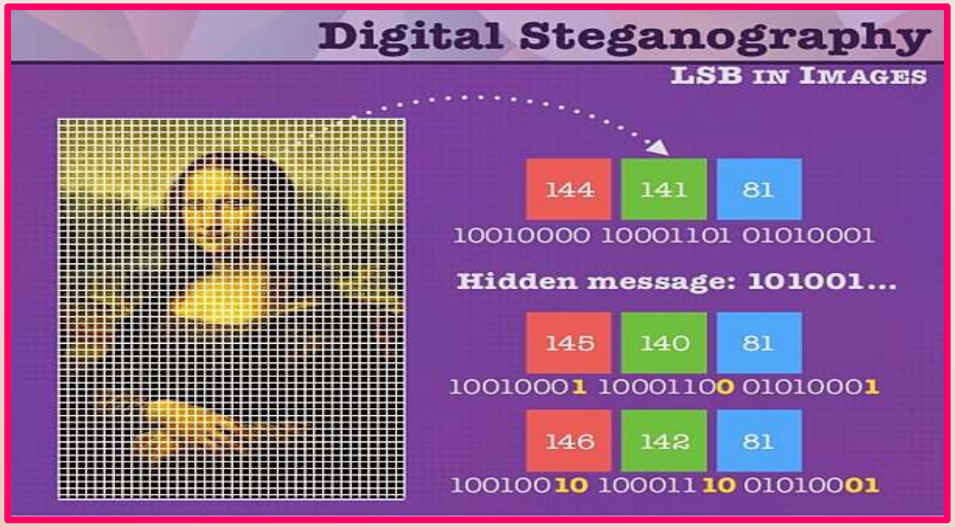
TERMS & DEFINITION

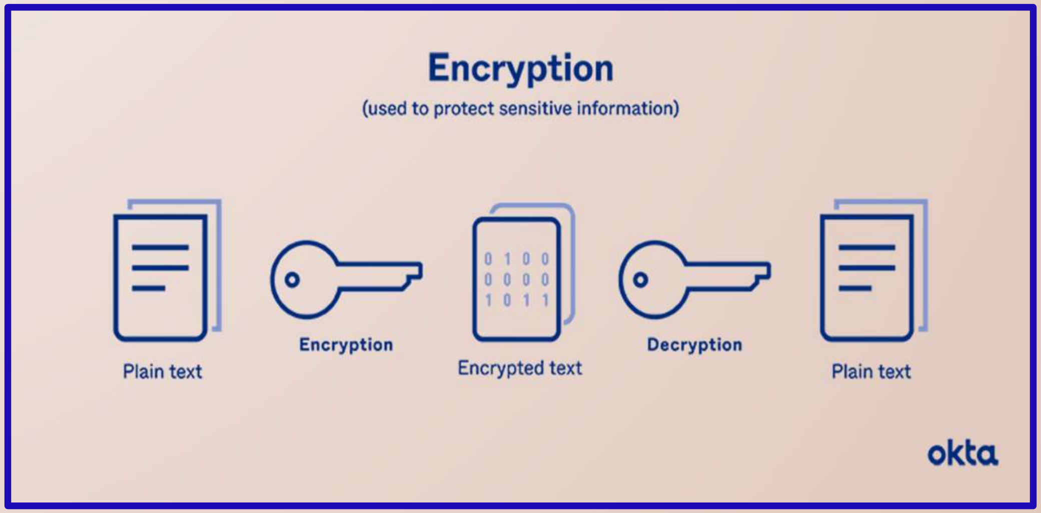
3. Steganography

- The art of hiding the existence of a message
- Ensures confidentiality & Integrity of a message
- **Example:** In a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image.

4. Encryption

- A method by which the information is converted into a secret code that hides the information’s true meaning. The science of encrypting and decrypting information is called c**ryptography.**



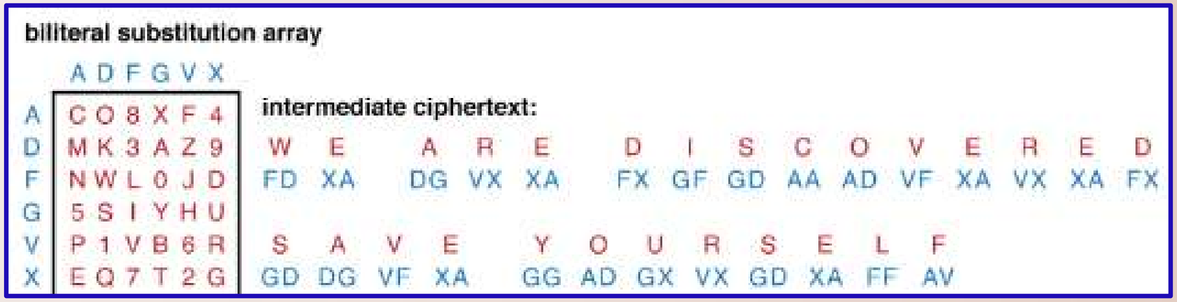


INFORMATION SECURITY - TERMS

TERMS & DEFINITION

5. Cipher

- Any method of transforming a message to conceal its meaning.
- Also used synonymously with ciphertext or cryptograms in reference to the encrypted form of a message



biliteral substitution array

	A	D	F	G	V	X
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	0	J	D
G	5	S	I	Y	H	U
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

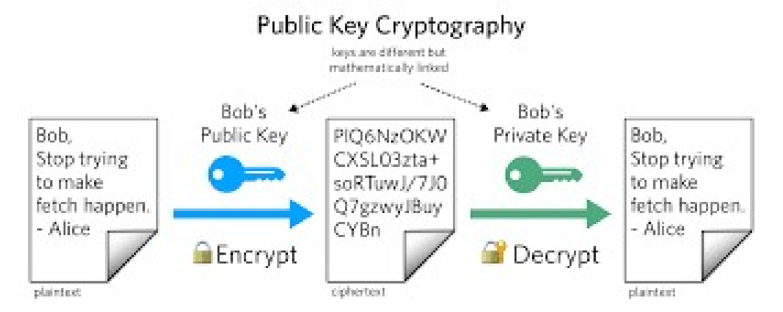
intermediate ciphertext:

W	E		A	R	E		D	I	S	C	O	V	E	R	E	D
FD	XA		DG	VX	XA		FX	GF	GD	AA	AD	VF	XA	VX	XA	FX

S	A	V	E		Y	O	U	R	S	E	L	F
GD	DG	VF	XA		GG	AD	GX	VX	GD	XA	FF	AV

6. Cryptography

- Cryptography refers to protecting information and communication through the use of codes so that only those for whom the information is intended can read and process it.


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSLO3zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

7. Cryptanalysis

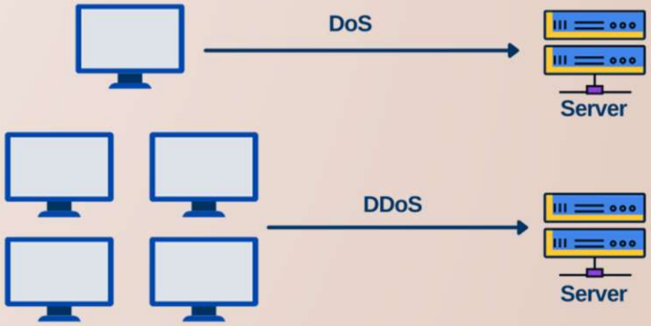
- Being able to break the cipher so that encrypted messages can be read

INFORMATION SECURITY - TERMS

TERMS & DEFINITION

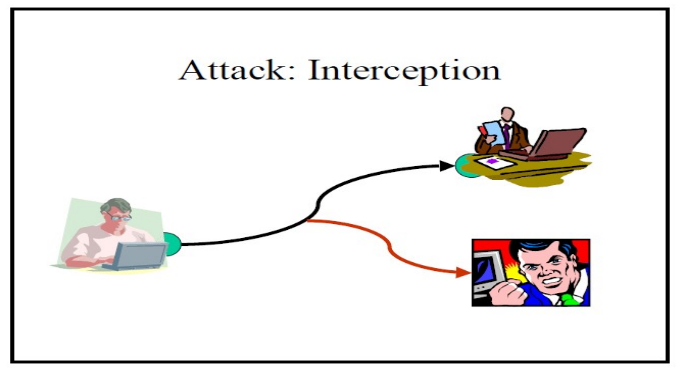
8. DOS ATTACK

- It is an attack meant to **shut down a machine** or **network**, making it inaccessible to its intended users
- It accomplishes this by **flooding the target with traffic** or **sending it information** that triggers a crash



9. Interception

- An **unauthorized party** gains access to an asset. Attack on confidentiality
- **Party** ⇒ may be a person, a program, or a computing system

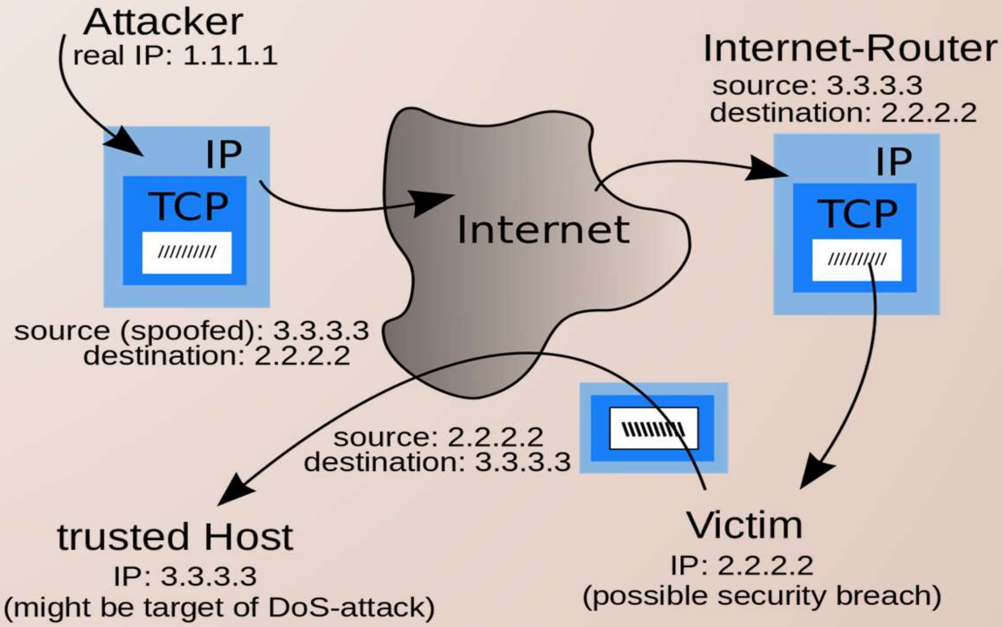


INFORMATION SECURITY - TERMS

TERMS & DEFINITION

10. Spoofing

- It is an attack in which a **malicious person** impersonates another device or uses on a network in order to launch an attack against **network hosts**, **steal data**, **spread malware,** or bypass access control
- In other words: when **someone** or **something** pretends to be **something else** in an attempt to gain a **victim's confidence**, **gain access to a system**, **steal data** or **spread malware**



INFORMATION CLASSIFICATIONS

Levels of Classification of Information

1. Unclassified 2. Sensitive but Unclassified 3. Confidential 4. Secret 5. Top Secret

UNCLASSIFIED

- The information that is neither sensitive nor classified. The public release of this information does not violate confidentiality

SENSITIVE BUT UNCLASSIFIED

- Information that has been designated as minor secret, but may **not create serious damage** if disclosed.

CONFIDENTIAL

- Information that is designated to be of a confidential nature. The disclosure can **lead to some damage** to national security.

SECRET

- Information that is designated to be a secret in nature. The disclosure can **lead to serious damage** to national security.

TOP SECRET

- The highest level of information classification. Its disclosure will cause exceptionally **grave damage** to the country’s national security.

INFORMATION CLASSIFICATIONS

Need to Know based Information Classification

1. Public 2. Sensitive 3. Private

PUBLIC

- Information that is similar to the unclassified information
- The unauthorized disclosure, alteration, or destruction of this data would result in little or no risk to the company

SENSITIVE

- Information requiring a **higher level of classification than normal data**.
- The **unauthorized disclosure**, **alteration**, or **destruction of that data** could cause a significant level of risk to the company.
- **Confidentiality** and **Integrity** need to be taken care of.

PRIVATE

- Information that is personal in nature and is intended for company use only.
- Disclosure of this data can adversely affect the company or its employees.
- **Basic examples include: Salary Levels** and **Medical information**

INFORMATION CLASSIFICATIONS

Criteria for Classification of Data and Information

1. Value 2. Age 3. Useful Life 4. Personal Association

VALUE

- The most commonly used criteria for classifying data in the private sector.
- If the information is valuable to an organization or its competitors, it needs to be classified.

AGE

- The classification of the information may be lowered if the information value decreases over time.
- In the Department of Defence some classified documents are automatically declassified after a predetermined time period has passed

USEFUL LIFE

- If the information has been made obsolete owning to new information, Substantial changes in the company or other reasons, the information can often be declassified

PERSONAL ASSOCIATION

- If the information is personally associated with specific individuals or is addressed by privacy law, it may need to be classified. For example, investigative information that reveals an informative name may need to remain classified.

INFORMATION CLASSIFICATIONS

Roles

1. Owner **2. Custodian** **3. User**

1. OWNER

- Executive or manager of an organization
- The owner has the final corporate responsibility for **data protection**, and under the concept of due care the owner may be liable for negligence because of the failure to protect these data.

Responsibilities of Owner

1. **Making the original decision** as to what level of classification the information requires based on the business needs for the protection of the data
2. **Reviewing the classification assignments periodically** and making alterations as the business needs to change
3. Delegating the responsibilities of the data protection **duties to a custodian**.

INFORMATION CLASSIFICATIONS

Roles

1. Owner **2. Custodian** **3. User**

2. CUSTODIAN

- ➢ It has operational responsibility for the physical and electronic security of the information

Responsibilities of Custodian

1. Running **regular backups** and **routinely testing** the validity of backup data.
2. Performing **the data restoration** from the backups when necessary.

3. USER

- ➢ They can be **operators**. They can be **system employees** or **external parties** that routinely use the information as a part of their job. Also, be called the **consumers of the data**.

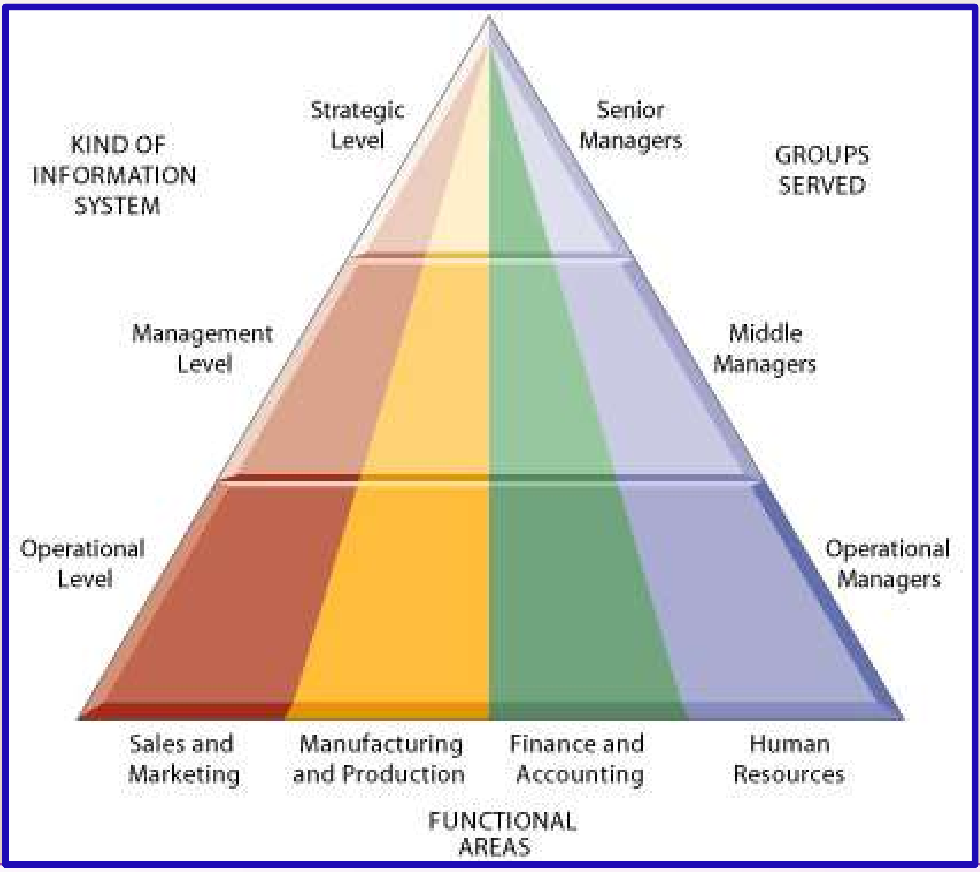
Responsibilities of User

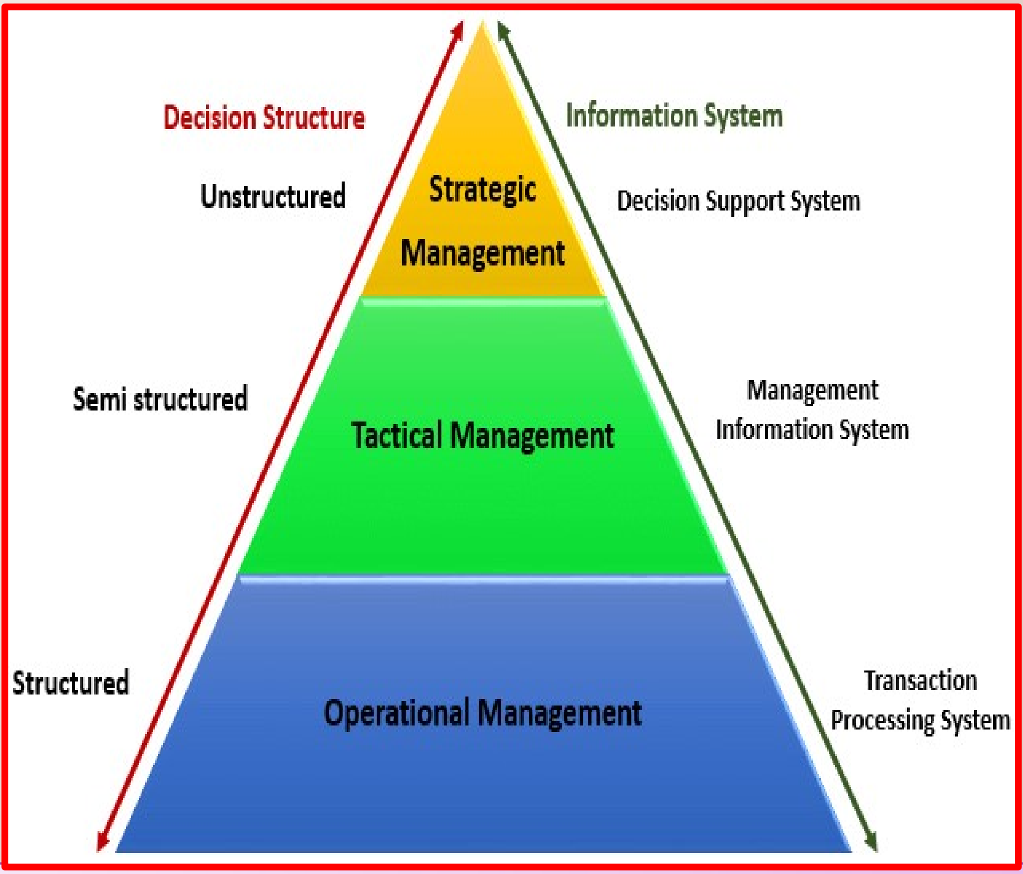
1. Follow the **operational procedures** that are defined by the organization's security policy and they must adhere to published guidelines for their use.
2. They must preserve **information security** during their work
3. They must prevent **"open view"** from occurring
4. They must use **companies' resources** only for company purposes and not for personal use.

INFORMATION SYSTEM - TYPES

Introduction

1. The typical organization is basically divided into 3 types. They are:
   a. Operational,
   b. Middle, and
   c. Upper Level





INFORMATION SYSTEM - LEVELS

Introduction

1. The typical organization is basically divided into 3 types.

   a. **Operational Level**

   - Concerned with performing day-to-day business transactions of the organization.
   - **Examples:** Cashier at a point of sale, bank tellers, nurses in a hospital, customer care staff, etc.

   b. **Organizational Level**

   - It is dominated by **middle-level managers**, **heads of the departments**, **supervisors**, etc.
   - The users at this level usually oversee the activities of the users at the operational management Level
   - **Example:** A **tactical manager** can check the **credit limit** and **payment history** of a customer and decide to make an exception to **raise** the credit limit for a particular customer.

   c. **Strategic Management Level**

   - It is the most **senior level** in an organization.
   - The user at this level makes the unstructured decision. Senior level managers are concerned with the long-term planning of the organization

INFORMATION SYSTEM - TYPES

Types

1. Information system is basically classified into 4 types:
   a. **Transactional Processing Systems (TPS)**
   b. **Management Information System (MIS)**
   c. **Decision Support System (DSS)**
   d. **Expert System**

Transactional Processing Systems (TPS)

➢ It is an information system that processes data resulting from the occurrences of business transactions.

➢ The main objective is to provide transactions in order to update records and generate reports i.e. to perform storekeeping functions.

➢ The transaction is performed in two ways:

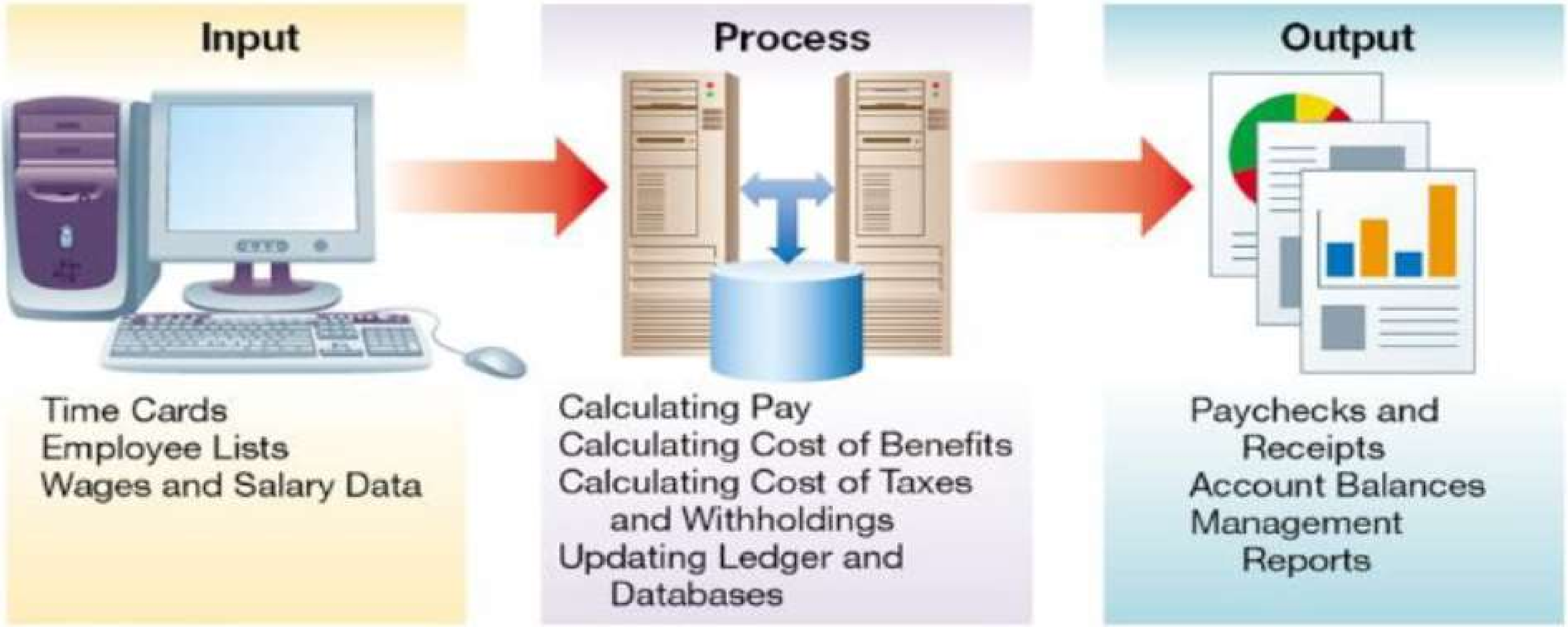
✓ **Batch processing** ⇒ In this transaction data is accumulated over a period of time and processed periodically.

✓ **Online Transaction Processing** ⇒ In this, the transaction data is processed immediately after they are generated and can provide immediate output to end users.

Examples: Bill System, Payroll System, Stock Control System

INFORMATION SYSTEM - TYPES

TPS Payroll System



Input

Time Cards
Employee Lists
Wages and Salary Data

Process

Calculating Pay
Calculating Cost of Benefits
Calculating Cost of Taxes and Withholdings
Updating Ledger and Databases

Output

Paychecks and Receipts
Account Balances
Management Reports

Payroll system shown as an instance of the basic systems model.

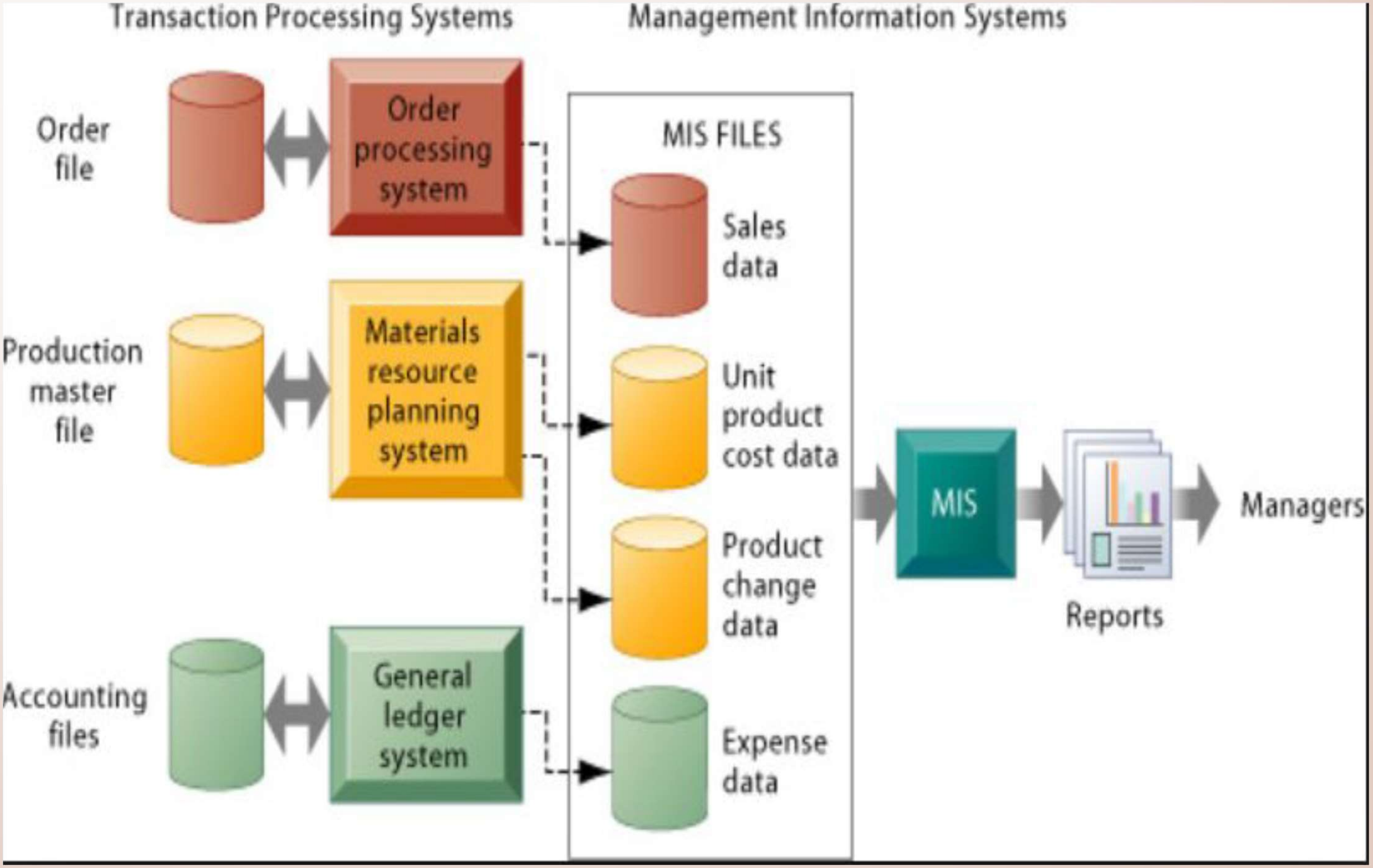
INFORMATION SYSTEM - TYPES

Management Information System (MIS)

- ➢ It is designed to take relatively raw data available through a Transaction Processing System (TPS) and convert them into a summarized and aggregated form for the manager, usually a report format.
- ➢ It reports tending to be used by middle management and operational supervisors
- ➢ Many different types of reports are produced in MIS. Some of them are:
  - ✓ **Summary Report**
  - ✓ **On-Demand Report**
  - ✓ **Ad-Hoc Report**
  - ✓ **Exception Report**

Examples: Sales Management System, Human Resource Management System

INFORMATION SYSTEM - TYPES



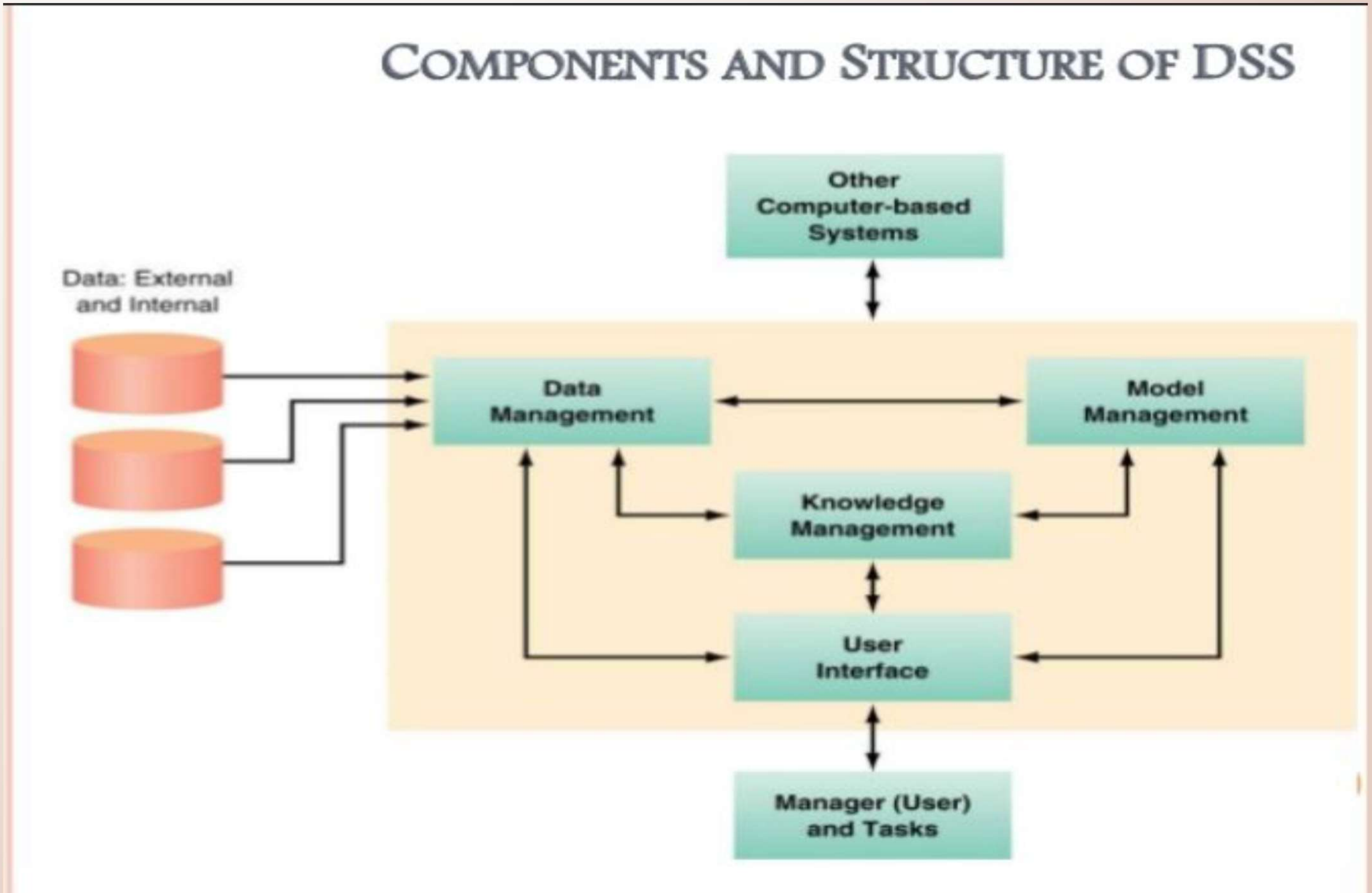
INFORMATION SYSTEM - TYPES

Decision Support System (DSS)

- It is an interactive information system that provides information, model and data manipulation tools to help in making the decision in a semi-structured and un-structured situation.
- It comprises of tools and techniques that help in gathering relevant information and analyse the options and alternatives, the end user is more involved in creating DSS than an MIS

Examples: Financial Planning System, Bank Loan Management System

INFORMATION SYSTEM - TYPES



INFORMATION SYSTEM - TYPES

Experts System (ES)

- It includes expertise in order to aid managers in diagnosing problem or in-problem solving.
- They are based on the principles of artificial intelligence research.
- Expert system is a knowledge based information system. It uses its knowledge to act as an expert consultant to the users.
- Knowledge base and software modules are the components of an expert system. These modules perform inference on the knowledge and offer answer to the user questions.

INFORMATION SYSTEM - SECURITY THREAT

Introduction to Security Threat

- When the information is leaked from the network or under the network is termed a **Security Threat.**
- It usually takes a toll on the **database** of the companies, leading to significant financial losses and confidential information leakage.
- **Data breach** is one of the most common problems experienced by companies.
- The threat can be caused by both the **internal** and **external** forces.

Security Threat Types

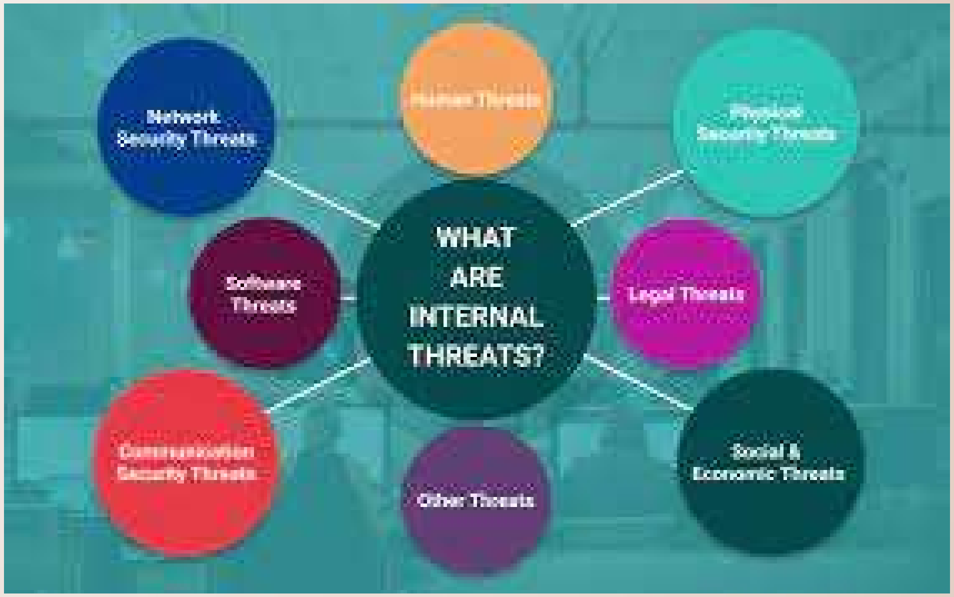
- **Internal Security Threat**
- **External Security Threat**
- **Unstructured Security Threat**
- **Structured Security Threat**

INFORMATION SYSTEM - SECURITY THREAT

Security Threat Types

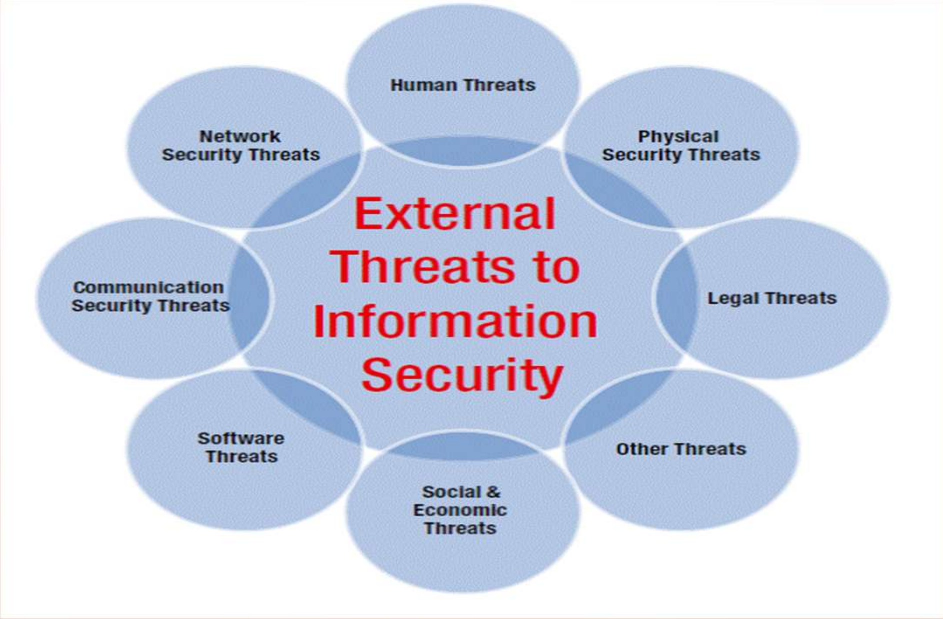
1. Internal Security Threat

- When the information is being leaked inside the network is Internal Security Threat
- 60% of the security threats are due to the internal security threat


Network Security Threats
Human Threats
Physical Security Threats
Software Threats
WHAT ARE INTERNAL THREATS?
Legal Threats
Communication Security Threats
Other Threats
Social & Economic Threats

2. External Security Threats

- When the information is being leaked outside the network is an External Security Threat
- This threat is detected by **IDS (Intrusion Detection System)**


Human Threats
Network Security Threats
Physical Security Threats
External Threats to Information Security
Communication Security Threats
Legal Threats
Software Threats
Other Threats
Social & Economic Threats

INFORMATION SYSTEM - SECURITY THREAT

Security Threat Types

3. Unstructured Security Threats

- Created by an inexperienced individual or the information leaked from the network by an inexperienced individual
- It often involves unfocused assaults on one or more network systems, often by individuals with limited or developing skills.
- The systems being attacked and infected are probably unknown to the perpetrator.
- These attacks are often the result of people with limited integrity and too much time on their hands.
- Malicious intent might or might not exists, but there is always indifference to the resulting damage caused to others.

INFORMATION SYSTEM - SECURITY THREAT

Security Threat Types

4. Structured Security Threats

- Created by an experienced individual or the information leaked from the network by an experienced individual
- It is more focused by one or more individuals with higher skills actively working to compromise a system.
- The targeted system could have been detected through some random search process or it might have been selected specifically.
- The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives.

INFORMATION SYSTEM - SECURITY THREAT

Security Threat Types

4. Structured Security Threats

- Created by an experienced individual or the information leaked from the network by an experienced individual
- It is more focused by one or more individuals with higher skills actively working to compromise a system.
- The targeted system could have been detected through some random search process or it might have been selected specifically.
- The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives.

INFORMATION SYSTEM - SECURITY THREAT

Security Threat Types

4. Structured Security Threats

- Created by an experienced individual or the information leaked from the network by an experienced individual
- It is more focused by one or more individuals with higher skills actively working to compromise a system.
- The targeted system could have been detected through some random search process or it might have been selected specifically.
- The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives.

INFORMATION SECURITY & RISK ANALYSIS

What is Risk?

1. It is basically made up to two parts:
   - ✓ The probability of something going wrong
   - ✓ The negative consequences if it does.

Risk Definition

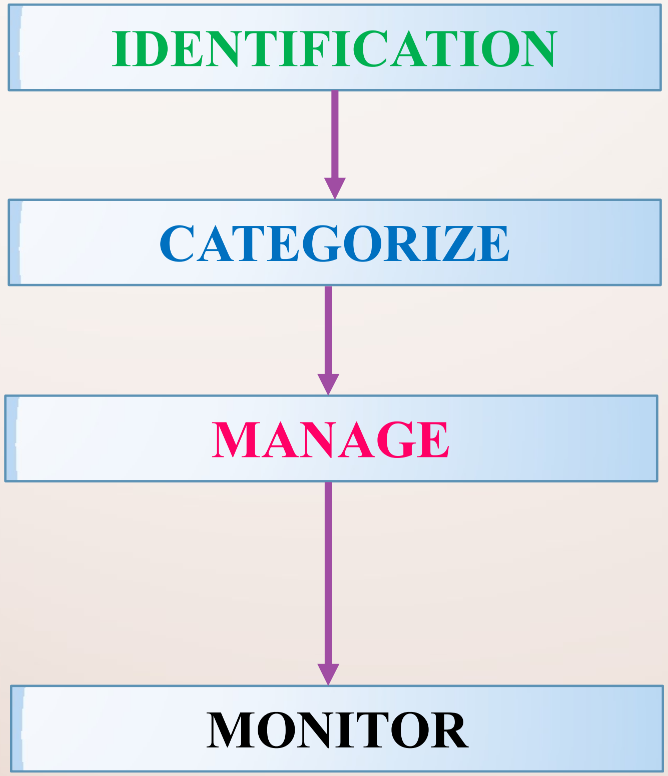
- ➢ It refers to the potential for loss or damage when a threat exploits a vulnerability.
- ➢ **Examples:** Includes financial losses as a result of:
  - ✓ business disruption,
  - ✓ loss of privacy,
  - ✓ reputational damage, and
  - ✓ legal implications and can even include loss of life.
- ➢ Risk can also be defined as follows:

Risk = Threat* X *Vulnerability

- ➢ The potential for risk can be reduced by creating and implementing a risk management plan.

INFORMATION SECURITY & RISK ANALYSIS

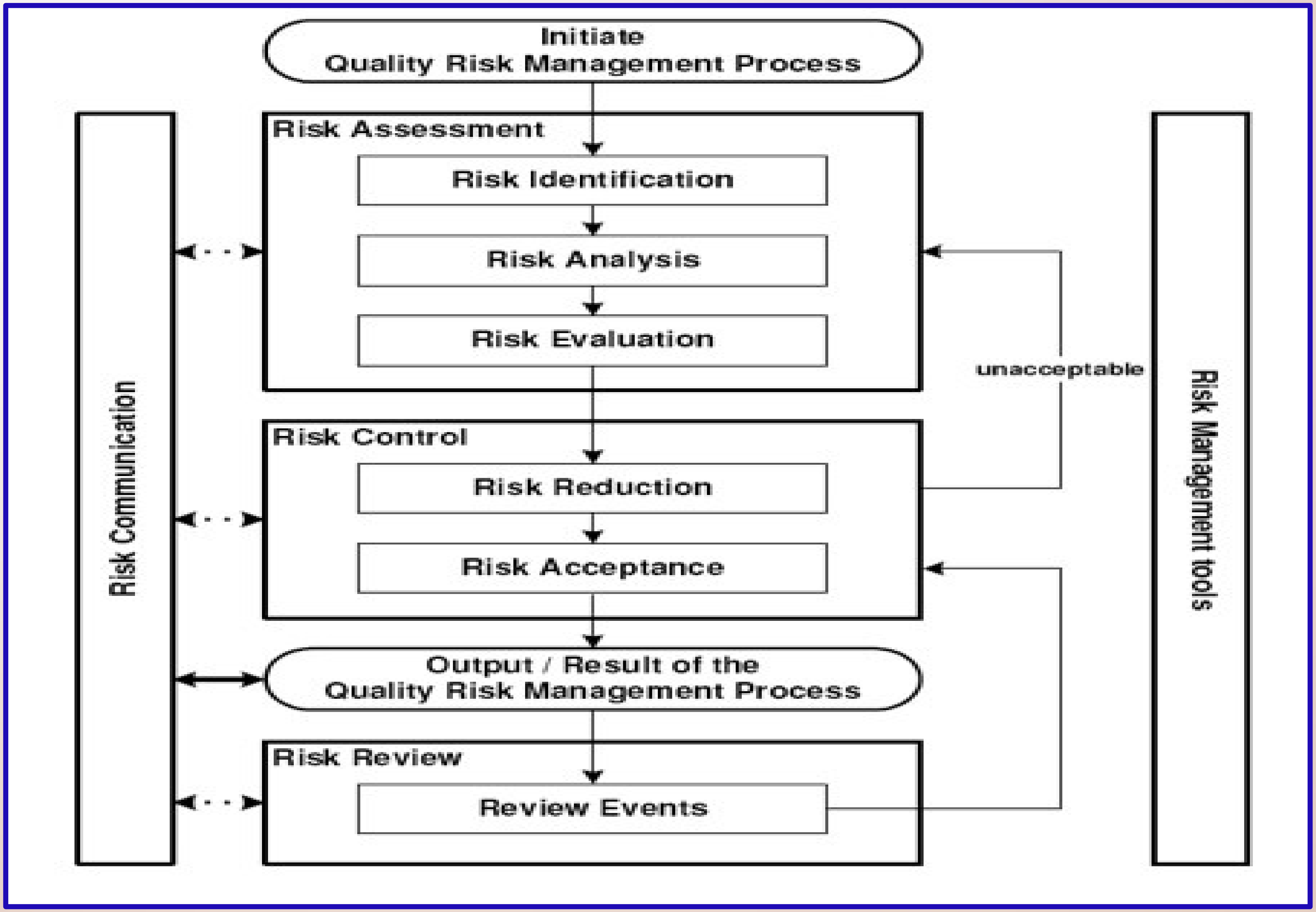
Risk Management Process



- Makes note of all possible risks, that may occur
- Categorize known risks into risk intensity as per their possible impact [High, Low, Medium]
- Analyse the probability of occurrence of risks at various phases.
- Make plans to avoid or face risks and attempt to minimize their side efforts.
- Closely monitor the potential risks and their earlier symptoms.
- Also monitor the effects of steps taken to mitigate or avoid them

INFORMATION SECURITY & RISK ANALYSIS

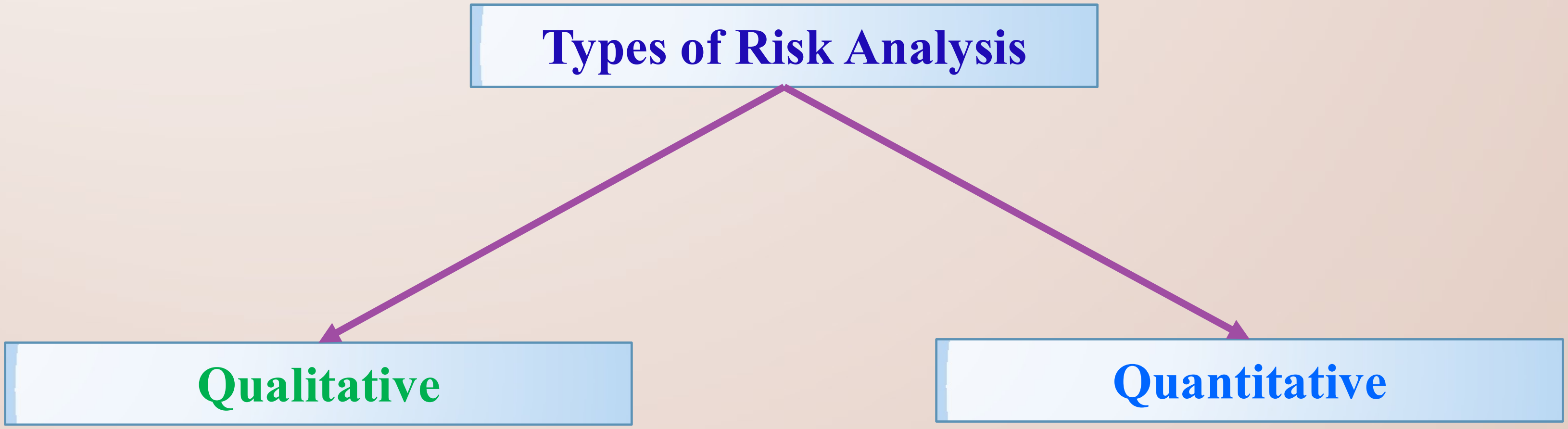
Risk Management Process



INFORMATION SECURITY & RISK ANALYSIS

What is Risk Analysis?

1. It is a **systematic process** to estimate the level of risk for identified and approved risks. This involves **estimating the probability** of **occurrence** and **consequences** of occurrence and converting the results to a corresponding risk.
2. It is the process of **defining** and **analyzing** the dangers to **individuals**, **businesses**, and **government agencies** posed by **potential natural** and **human-caused** adverse events.
3. Risk analysis is the process of **identifying** and **analyzing** potential issues that could negatively impact **key business initiatives** or **critical projects** in order to help organizations avoid or mitigate those risks



INFORMATION SECURITY & RISK ANALYSIS

Qualitative Risk Analysis

1. It aids in **accessing** and **evaluating** the characteristics of the **identified risk** and prioritizing them accordingly.
2. It prioritizes the **identified risks** using a **pre-defined rating scale**.
3. **Risks** will be scored based on their **probability** or **likelihood** of occurring and their impact.
4. It is necessary after risk factors have been identified.

Example:

- Qualitative analysis would use a scale of "**Low, Medium**, **High**" to indicate the likelihood of a **risk** event occurring.
- For **example**, **Risk** #1 has an 80% chance of occurring, **Risk** #2 has a 27% chance of occurring, and so on.

Advantages: easy to understand, provide an adequate indication of the organization’s security risk

Disadvantages: subject to, may not be trusted by some in management positions

INFORMATION SECURITY & RISK ANALYSIS

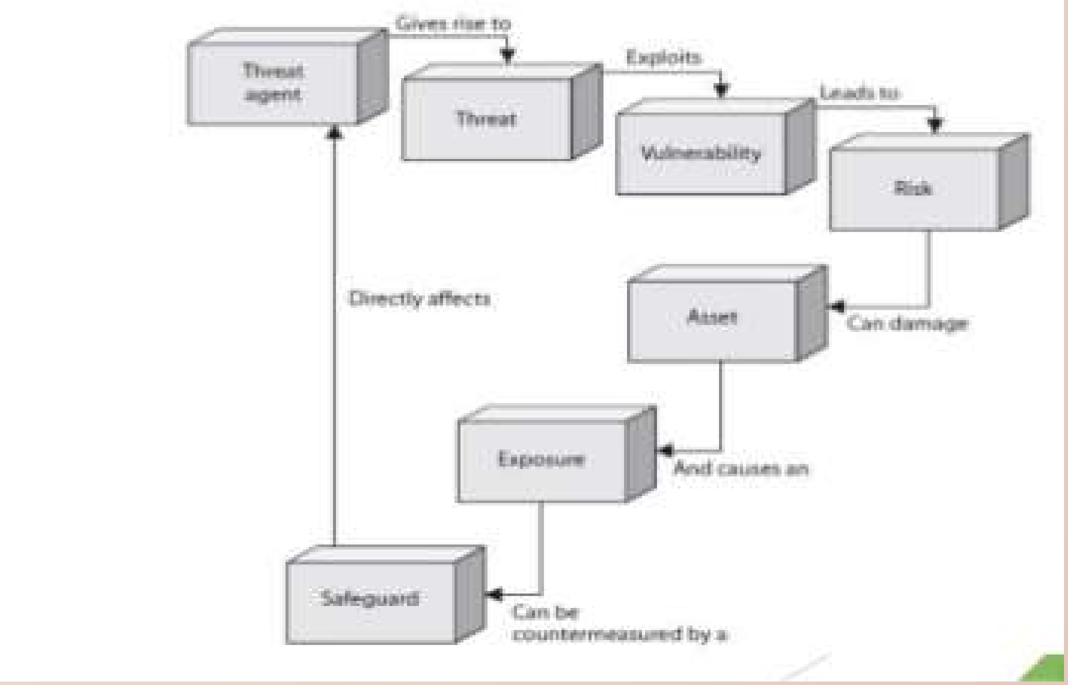
Quantitative Risk Analysis

1. It provides a **numerical estimate** of the overall effect of risk on the objectives of the project.
2. It helps in calculating estimates of overall risk which is the main focus.
3. Provides a numeric estimate of the probability of **risk** and the magnitude of the consequences.

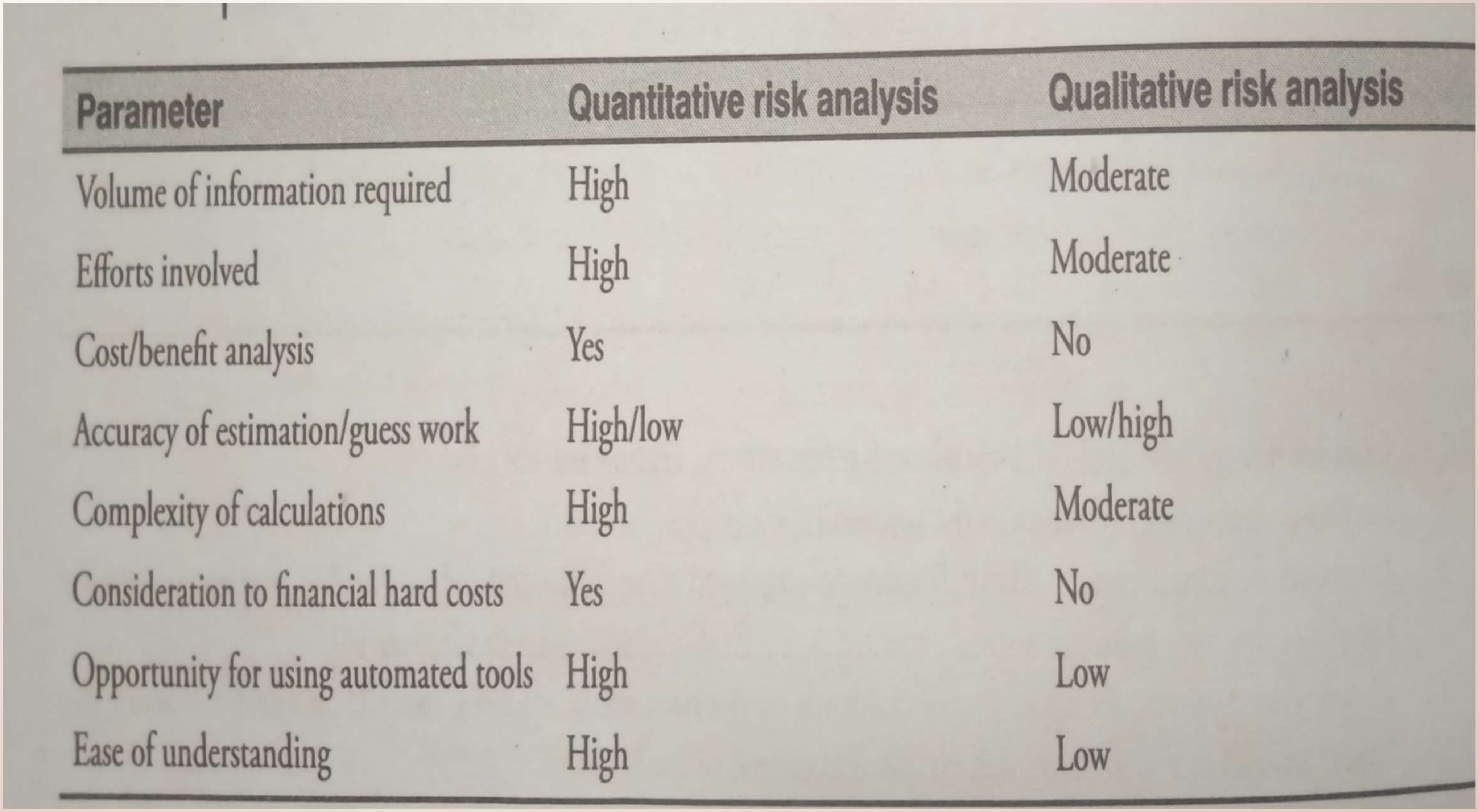
Advantages: objective, security risk expressed in terms of dollar

Disadvantages: security risk calculations are complex, and accurate values are difficult to obtain

Relationship Among Different Security Concepts



INFORMATION SECURITY & RISK ANALYSIS



Parameter	Quantitative risk analysis	Qualitative risk analysis
Volume of information required	High	Moderate
Efforts involved	High	Moderate
Cost/benefit analysis	Yes	No
Accuracy of estimation/guess work	High/low	Low/high
Complexity of calculations	High	Moderate
Consideration to financial hard costs	Yes	No
Opportunity for using automated tools	High	Low
Ease of understanding	High	Low

INFORMATION SECURITY & RISK ANALYSIS

Terms and Definition of Risk Analysis

1. **Asset**
   - Something that an organization considers important so as to be protected.
   - **Examples:** a resource, process, product, computing infrastructure, etc.
   - The loss of the asset could affect the **CIA** or could have an overall adverse business impact.
2. **Threat**
   - It is the presence of any potential event that could cause an adverse impact on the organization.
3. **Safeguard**
   - A safeguard is the ‘control’ or ‘countermeasure’ put in place to reduce the risk associated with a specific threat or group of threats.
4. **Vulnerability**
   - The absence or weakness of a ‘**safeguard**’.
   - A minor threat has the potential to become a greater threat because of vulnerability.

INFORMATION SECURITY & RISK ANALYSIS

Exposure Related Terms

1. **Exposure Factor (EF)**
   - Represents a **percentage loss** that a threat event would have on a **specific asset**.
   - The EF values are needed to compute the **single loss expectancy(SLE)**. SLE intern is necessary to compute the **annualized loss expectancy(ALE)**
   - Exposure Factor can be a **small percentage** such as the effect of **loss of some hardware** (or) a very **large percentage** such as **loss of storage devices at some data center**
2. **Single Loss Expectancy (SLE)**
   - A **monitory figure** that is assigned to a single threat event. It represents an organization's loss from a single threat.

SLE = Asset_Value (in monetary terms) * EF

Example: Asset Value = 45000$, EF = 20% then SLE = (45000*0.2) ⇒ 900$

3. **Annualized Rate of Occurrence (ARO)**
   - It represents the estimated probability of a specific threat taking place within a one-year time frame. The rate of probability is from 0.0 to 1.0

Example: Probability of flood is once in 1000 years, ARO value will be 0.001

INFORMATION SECURITY & RISK ANALYSIS

Exposure Related Terms

4. Annualized Loss Expectancy (ALE)

- It is a monetary value derived from **ALE = SLE * ARO**

Formula For Risk Analysis

Exposure-Related Concept	Formula for Calculation
Exposure factor(EF)	Percentage of asset loss caused by a threat
Single loss expectancy(SLE)	Asset value * EF
Annualized rate of occurrence(ARO)	Frequency of threat occurrence per year
Annualized loss expectancy(ALE)	SLE * ARO

RISK MANAGEMENT & RISK ANALYSIS

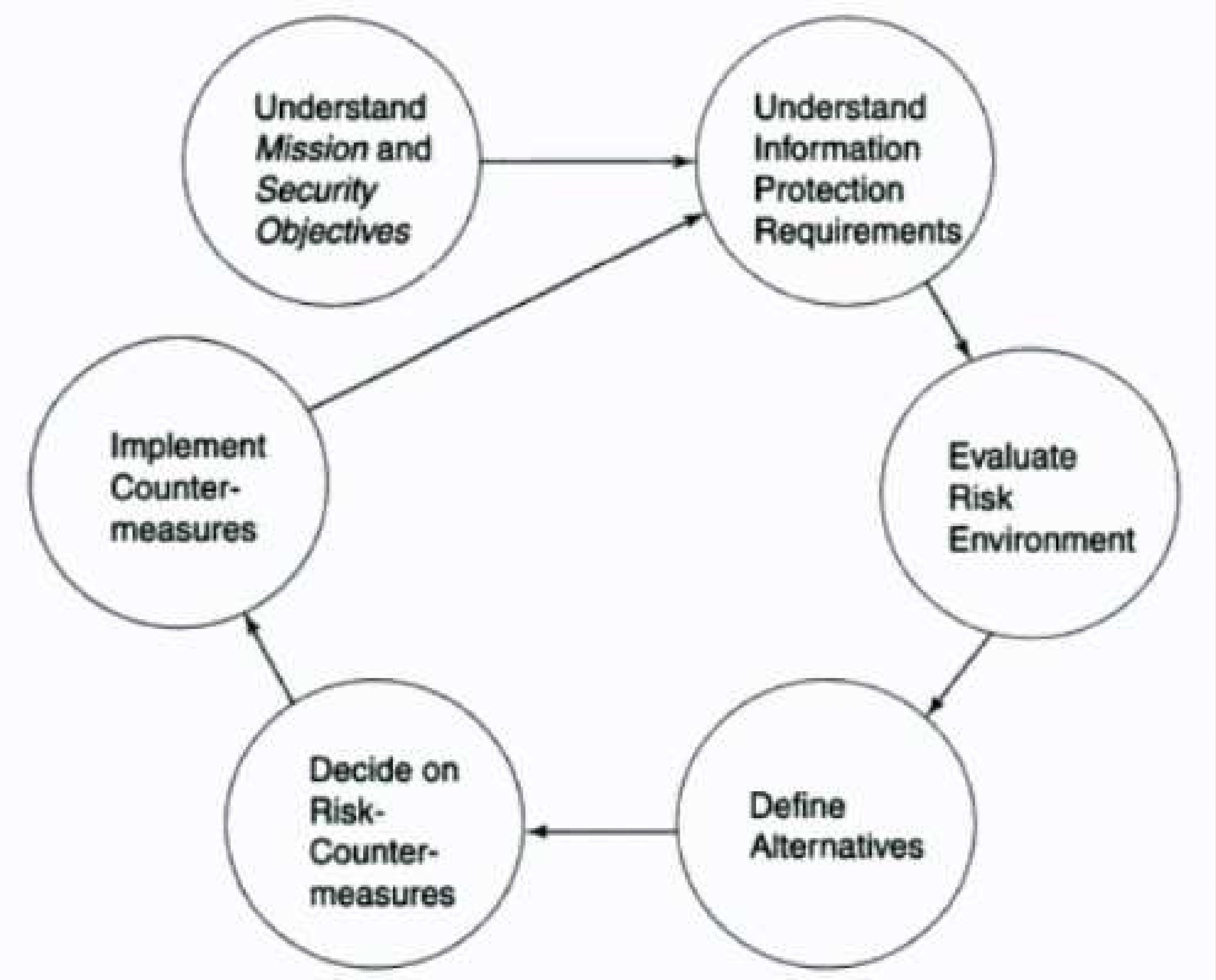
Introduction

1. **Risk Analysis**
   - Signs of observation, knowledge, and evaluation
   - It is the keystone to effective performance as well for targeted, proactive solutions to potential threats and incidents
2. **Risk Management**
   - The ongoing process of identifying the risk and implementing plans to address them.
   - Skill of handling the identified risk in the best possible manner for the interest of the organization
3. **Risk Evaluation**
   - Provides a baseline that can be used to focus mitigation and improvement activities
   - It is a process that generates an organization-wide view of infosec risk. It provides a baseline that can be used to focus mitigation and improvement activities
   - Many organizations employ staff to hold the post of "**chief risk officer**" for risk management

Risk = Threat * Vulnerability * Asset Value

RISK MANAGEMENT & RISK ANALYSIS

Process of Risk Analysis/Risk Management


Understand *Mission* and *Security Objectives*
Understand Information Protection Requirements
Evaluate Risk Environment
Define Alternatives
Decide on Risk-Counter-measures
Implement Counter-measures

RISK MANAGEMENT & RISK ANALYSIS

Staged Methodology for Risk Analysis

1. Methodology

- It is a **framework** for managing a task efficiently, usually including standard techniques for problem-solving.
- There are **three main stages** in risk analysis:
  - ✓ Asset evaluation
  - ✓ Analysis of threats and vulnerabilities
  - ✓ Selection of safeguards

Considerations for Risk Analysis

1. Valuation (estimation) of Assets
2. Selection of Safeguards

RISK MANAGEMENT & RISK ANALYSIS

Staged Methodology for Risk Analysis

1. Asset Evaluation

- ➢ Asset valuation is the calculation of the financial value of an organization's assets reported at the end of a financial period.
- ➢ The principal purpose of asset valuation is to produce the financial value of the highway infrastructure assets owned by an organization to put on the organizations balance sheet

2. Asset Classification

- ➢ An asset is anything that the organizations consider as a key component of their business process
- ➢ Asset classification is necessary for asset evaluation
- ➢ Categories of information assets
  - ✓ Hardware & Software
  - ✓ Data & Documentation
  - ✓ Personal and procedures
  - ✓ Models and communication equipment
  - ✓ Logical datasets and intangible aspects such as business reputation

RISK MANAGEMENT & RISK ANALYSIS

Why Asset Evaluation is Required?

1. **Reason for Asset Evaluation**
   - As a basis for cost/benefits analysis
   - Insurance-related and other statutory requirements
   - For making decisions on the selection of safeguards
   - As a part of mandated do you care and to abide with legal requirements
2. **Number of Factors Considered while performing Asset Evaluation**
   - Usefulness and lifespan of the asset
   - Initial one-time cost of the asset
   - Ongoing operational cost of the asset
   - Maintenance support cost of the asset
   - Hidden costs associated with the asset
   - Value of the intellectual property

RISK MANAGEMENT & RISK ANALYSIS

Selection of Safeguards

1. After completion of risk analysis. The next step is to perform research on safeguards/ countermeasures for protecting critical information assets.
2. Many standard principles are used to ensure that the selected safeguards match the threat through either of the approaches to risk analysis - quantitative or qualitative
3. The selection of safeguards is done based on the following:
   - ✓ Cost/benefit analysis
   - ✓ Level of manual operations required
   - ✓ Auditability or accountability features of the safeguard
   - ✓ Ability for recovery