SMS3112: Information security and systems

INSTRACTOR. John
MUNYAKAYANZA
DEPT. INFORMATION SYSTEMS
NYARUGENGE –CAMPUS
CST-UNIVERSITY OF RWANDA

Contents

- Introduction
- Application of Information Security in Military Science
- Cryptography
- Network security
- Security polices, standards and procedures
- IDS
- Social Engineering Attacks
- Security Applications

Introduction

- Information system (IS):
  - A set of interrelated components that collect, manipulate, and disseminate data and information and provide feedback to meet an objective

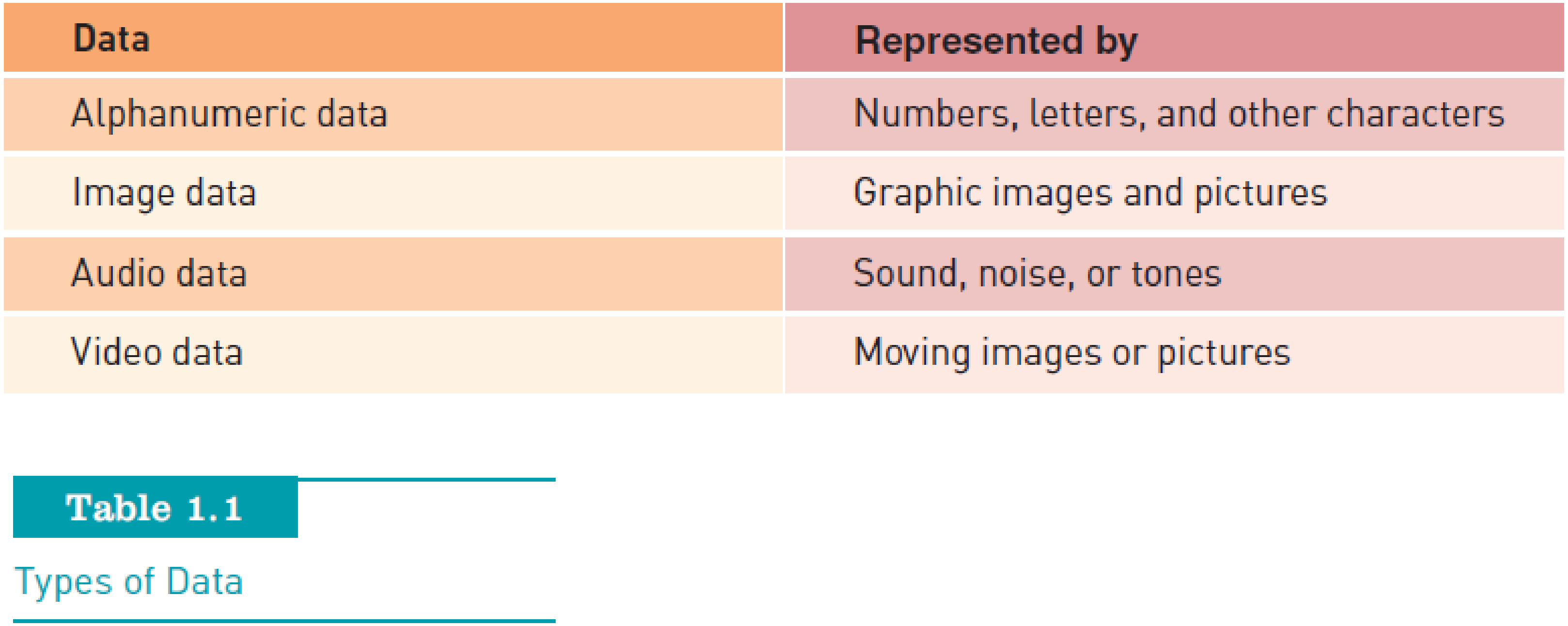
Information Concepts

- Information:
  - One of an organization’s most valuable resources
  - Often confused with the term *data*

Data, Information, and Knowledge

- Data:
  - Raw facts
- Information:
  - Collection of facts organized in such a way that they have value beyond the facts themselves
- Process:
  - Set of logically related tasks
- Knowledge:
  - Awareness and understanding of a set of information

Data, Information, and Knowledge (continued)

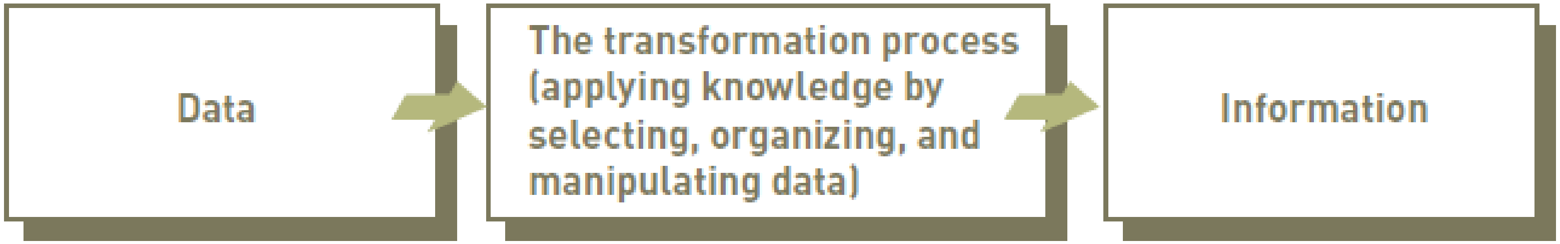


Data	Represented by
Alphanumeric data	Numbers, letters, and other characters
Image data	Graphic images and pictures
Audio data	Sound, noise, or tones
Video data	Moving images or pictures

Table 1.1

Types of Data

Data, Information, and Knowledge (continued)



Data

The transformation process (applying knowledge by selecting, organizing, and manipulating data)

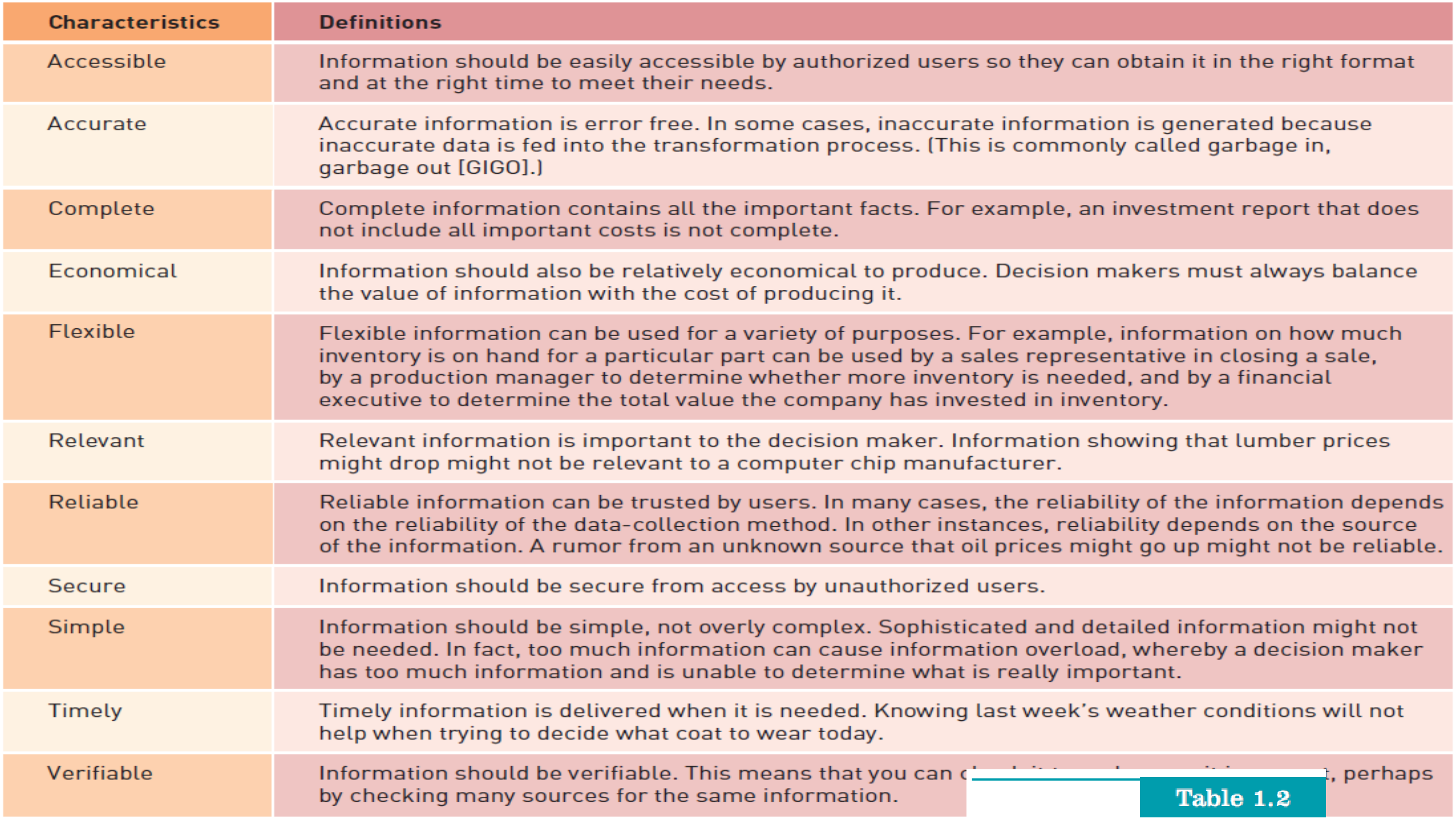
Information

Figure 1.2

The Process of Transforming Data into Information

The Characteristics of Valuable Information

- If an organization’s information is not accurate or complete:
  - People can make poor decisions, costing thousands, or even millions of dollars
- Depending on the type of data you need:
  - Some characteristics become more important than others



Characteristics	Definitions
Accessible	Information should be easily accessible by authorized users so they can obtain it in the right format and at the right time to meet their needs.
Accurate	Accurate information is error free. In some cases, inaccurate information is generated because inaccurate data is fed into the transformation process. (This is commonly called garbage in, garbage out [GIGO].)
Complete	Complete information contains all the important facts. For example, an investment report that does not include all important costs is not complete.
Economical	Information should also be relatively economical to produce. Decision makers must always balance the value of information with the cost of producing it.
Flexible	Flexible information can be used for a variety of purposes. For example, information on how much inventory is on hand for a particular part can be used by a sales representative in closing a sale, by a production manager to determine whether more inventory is needed, and by a financial executive to determine the total value the company has invested in inventory.
Relevant	Relevant information is important to the decision maker. Information showing that lumber prices might drop might not be relevant to a computer chip manufacturer.
Reliable	Reliable information can be trusted by users. In many cases, the reliability of the information depends on the reliability of the data-collection method. In other instances, reliability depends on the source of the information. A rumor from an unknown source that oil prices might go up might not be reliable.
Secure	Information should be secure from access by unauthorized users.
Simple	Information should be simple, not overly complex. Sophisticated and detailed information might not be needed. In fact, too much information can cause information overload, whereby a decision maker has too much information and is unable to determine what is really important.
Timely	Timely information is delivered when it is needed. Knowing last week's weather conditions will not help when trying to decide what coat to wear today.
Verifiable	Information should be verifiable. This means that you can c[illegible]t, perhaps by checking many sources for the same information.

Table 1.2

Characteristics of Valuable Information

The Value of Information

- Directly linked to how it helps decision makers achieve their organization’s goals
- Valuable information:
  - Can help people and their organizations perform tasks more efficiently and effectively

What is an Information System?

- Information system (IS) is a set of interrelated elements that:
  - Collect (input)
  - Manipulate (process)
  - Store
  - Disseminate (output) data and information
  - Provide a corrective reaction (feedback mechanism) to meet an objective

What is an Information System? (continued)

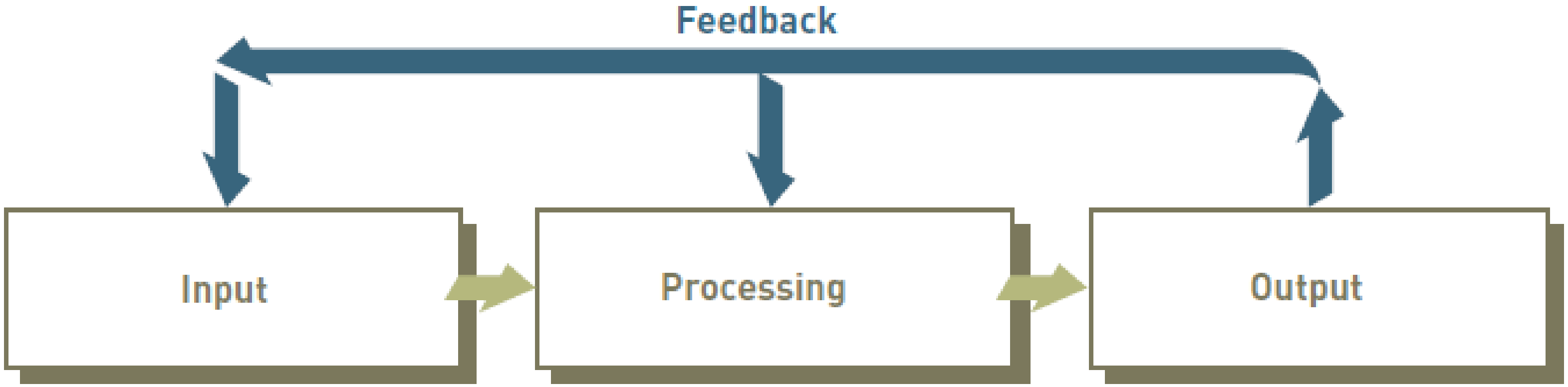


Figure 1.5

The Components of an Information System

Feedback is critical to the successful operation of a system.

Input, Processing, Output, Feedback

- Input:
  - Activity of gathering and capturing raw data
- Processing:
  - Converting data into useful outputs
- Output:
  - Production of useful information, usually in the form of documents and reports
- Feedback:
  - Information from the system that is used to make changes to input or processing activities

Manual and Computerized Information Systems

- An information system can be:
  - Manual or computerized
- Example:
  - Investment analysts manually draw charts and trend lines to assist them in making investment decisions

Computer-Based Information Systems

- Single set of hardware, software, databases, telecommunications, people, and procedures:
  - That are configured to collect, manipulate, store, and process data into information
- Technology infrastructure:
  - Includes all hardware, software, databases, telecommunications, people, and procedures
    - Configured to collect, manipulate, store, and process data into information

Computer-Based Information Systems (continued)

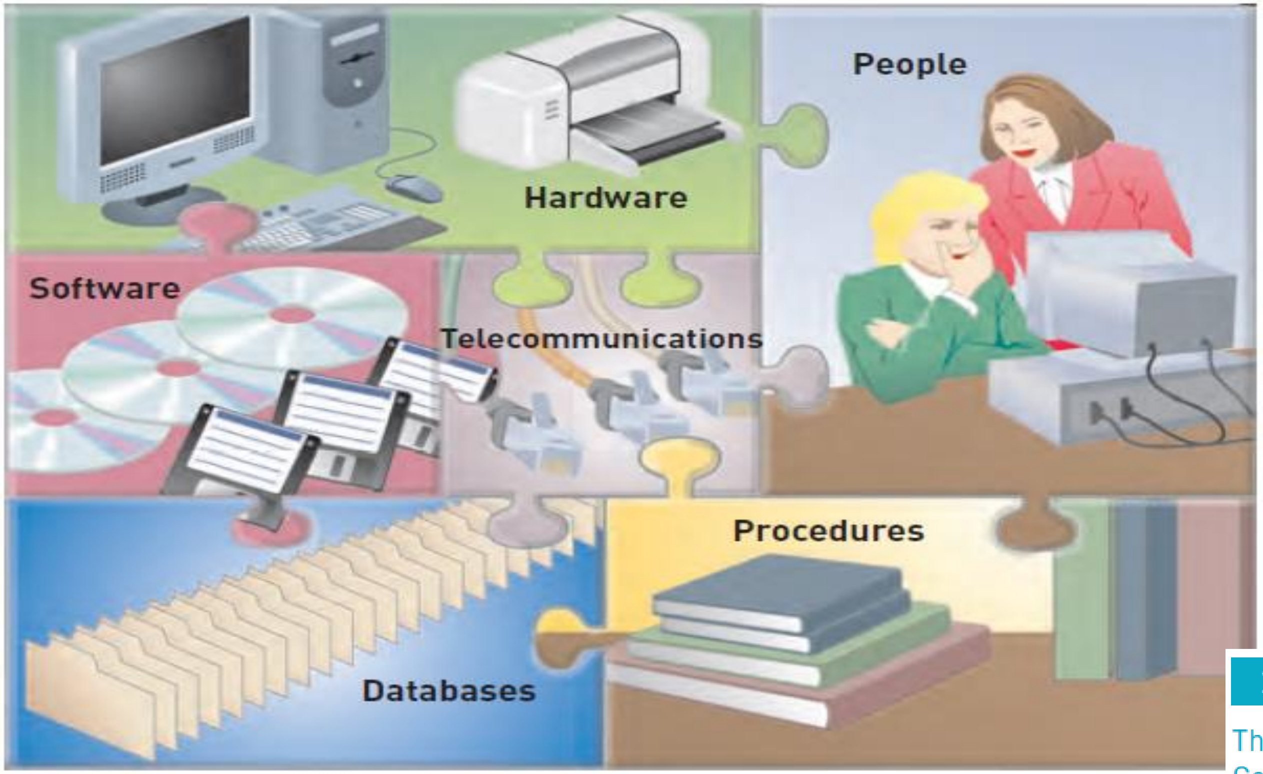


Figure 1.4

The Components of a Computer-Based Information System

Computer-Based Information Systems (continued)

- Hardware:
  - Consists of computer equipment used to perform input, processing, and output activities
- Software:
  - Consists of the computer programs that govern the operation of the computer
- Database:
  - Organized collection of facts and information, typically consisting of two or more related data files

Computer-Based Information Systems (continued)

- Telecommunications, networks, and the Internet:
  - The electronic transmission of signals for communications
- Networks:
  - Connect computers and equipment to enable electronic communication
- Internet:
  - World’s largest computer network, consisting of thousands of interconnected networks, all freely exchanging information

Computer-Based Information Systems (continued)

- Intranet:
  - Internal network that allows people within an organization to exchange information and work on projects
- Extranet:
  - Network that allows selected outsiders, such as business partners and customers, to access authorized resources of a company’s intranet

Computer-Based Information Systems (continued)

- People:
  - The most important element in most computer-based information systems
- Procedures:
  - Include strategies, policies, methods, and rules for using the CBIS

UNIVERSITY of RWANDA

Business Information Systems

- Most common types of information systems:
  - Those designed for electronic and mobile commerce, transaction processing, management information, and decision support
- Some organizations employ:
  - Special-purpose systems, such as virtual reality, that not every organization uses

Electronic and Mobile Commerce

- E-commerce:
  - Any business transaction executed electronically between:
    - Companies (business-to-business, B2B)
    - Companies and consumers (business-to-consumer, B2C)
    - Consumers and other consumers (consumer-to-consumer, C2C)
    - Business and the public sector
    - Consumers and the public sector

Electronic and Mobile Commerce (continued)

- Mobile commerce (m-commerce):
  - The use of mobile, wireless devices to place orders and conduct business
- E-commerce:
  - Can enhance a company’s stock prices and market value
- Electronic business (e-business):
  - Uses information systems and the Internet to perform all business-related tasks and functions

Information Security

- Definition of Information System Security: Information system security refers to the protection of information and the systems that store, process, and transmit that information from unauthorized access, use, disclosure, disruption, modification, or destruction.

- Importance of Information System Security: Information is a valuable asset for organizations, and ensuring its security is crucial to protect against various threats, safeguard sensitive data, maintain trust, comply with regulations, and avoid financial and reputational damage.

Objectives of Information System Security

- Confidentiality: Ensuring that information is accessible only to authorized individuals and remains confidential.
- Integrity: Maintaining the accuracy, consistency, and trustworthiness of information by preventing unauthorized modification or tampering.
- Availability: Ensuring that information and systems are available and accessible to authorized users when needed.

Common Threats to Information Systems

- Malware: Includes viruses, worms, ransomware, and other malicious software that can infect systems, compromise data, or disrupt operations.
- Social Engineering: Techniques such as phishing, pretexting, and impersonation aimed at manipulating individuals into revealing sensitive information or performing actions that compromise security.
- Insider Threats: Actions or misuse of privileges by authorized individuals within an organization that can result in unauthorized access, data breaches, or sabotage.
- Denial of Service (DoS) Attacks: Attempts to overwhelm or exhaust system resources, making services or information unavailable to legitimate users.
- Physical Theft or Damage: Unauthorized access, theft, or destruction of physical assets, such as servers, laptops, or storage devices, which can lead to data loss or system compromise

Information Security Principles

- Defense in Depth: Implementing multiple layers of security controls to provide redundancy and protection against various threats.
- Least Privilege: Granting individuals or systems the minimum necessary privileges and access rights to perform their tasks, reducing the potential for unauthorized actions.
- Separation of Duties: Assigning different responsibilities and tasks to different individuals to prevent a single person from having complete control and authority over critical systems or data.
- Access Control: Implementing mechanisms to authenticate and authorize users, ensuring that only authorized individuals can access specific resources.
- Risk Assessment and Management: Identifying and evaluating potential risks and implementing measures to mitigate or manage those risks effectively.

Security Controls

- Authentication: Verifying the identity of users or systems, often through passwords, biometrics, or two-factor authentication.
- Encryption: Protecting the confidentiality and integrity of data by converting it into an unreadable format using cryptographic algorithms.
- Firewalls: Network security devices that monitor and control incoming and outgoing traffic based on predetermined security rules.
- Intrusion Detection Systems (IDS): Monitoring systems or networks for suspicious or unauthorized activity and generating alerts or taking preventive measures.
- Security Awareness Training: Educating users about security best practices, potential risks, and how to identify and respond to security threats.

Security Policies and Procedures

Importance of Policies and Procedures: Establishing clear guidelines and rules for security practices, acceptable use of resources, incident response, and other security-related activities.

Examples of Security Policies: Password policy, acceptable use policy, incident response policy, data classification policy, remote access policy, etc.

Incident Response and Management: Defining procedures for detecting, responding to, and recovering from security incidents, including reporting, investigation, and communication processes

Compliance and Legal Considerations

- Regulatory Compliance: Adhering to industry-specific regulations and legal requirements, such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), or PCI DSS (Payment Card Industry Data Security Standard).
- Data Privacy and Protection: Protecting personally identifiable information (PII), sensitive data, and ensuring compliance with privacy laws.
- Intellectual Property Protection: Safeguarding intellectual property, trade secrets, patents, copyrights, and proprietary information from unauthorized access or theft.

Emerging Technologies and Trends

- Cloud Security: Addressing security challenges and considerations in cloud computing environments, such as data protection Emerging Technologies and Trends, access control, and secure integration with existing systems.
- Internet of Things (IoT) Security: Ensuring the security of interconnected devices, networks, and data generated by IoT devices, including privacy, data integrity, and device authentication.
- Artificial Intelligence (AI) and Machine Learning in Security: Utilizing AI and machine learning algorithms to enhance threat detection, anomaly detection, and security analytics.

Why do Learn Information Systems in Organizations?

- Information systems used by:
  - Sales representatives
  - Managers
  - Financial advisors
- Information systems:
  - Indispensable tools to help you achieve your career goals

Information and Decision Support Systems

- Management information system (MIS):
  - Organized collection of people, procedures, software, databases, and devices that provides routine information to managers and decision makers

Thank You

……..Murakoze…….!