RUZANNA BINTI JUBAIDI NORLELA BINTI ZAMAN
SITI AISHAH BINTI AB JALIL

MANAGEMENT INFORMATION SYSTEM: FUNDAMENTALS

FIRST EDITION

MANAGEMENT INFORMATION SYSTEM: FUNDAMENTALS

Ruzanna binti Jubaidi
Norlela binti Zaman
Siti Aishah binti Ab Jalil

Senior Lecturers
Politeknik Sultan Salahuddin Abdul Aziz Shah,
Shah Alam

MANAGEMENT INFORMATION SYSTEM: FUNDAMENTALS

AUTHORS:
Ruzanna binti Jubaidi
Norlela binti Zaman
Siti Aishah binti Ab Jalil

e ISBN 978-967-0032-91-7

First published: 2023

PUBLISHED BY:
UNIT PENERBITAN
Politeknik Sultan Salahuddin Abdul Aziz Shah
Persiaran Usahawan,
SeksyenU1,
40150 Shah Alam Selangor
Telephone No. : 03 5163 4000
Fax No. : 03 5569 1903

PREFACE

Information systems are a fundamental component of all business operations today. In this book, students are provided with a basic understanding of the role and significance of information systems. The book also addresses the ethical and security issues that are associated with the digital age.

Each chapter begins with a description of the learning outcomes. Students will be able to understand management information system concepts more clearly and will be able to use this book as a guide in preparing for their examinations. The approach of this book makes it an ideal resource for students enrolled in polytechnics.

Ruzanna binti Jubaidi
Norlela binti Zaman
Siti Aishah binti Ab Jalil

ACKNOLEDGEMENT

Throughout the review process, our reviewers provided spirited comments and suggestions that contributed significantly to the publication of this e-book. Our sincere thanks go out to everyone at Politeknik Sultan Salahuddin Abdul Aziz Shah who contributed to the development of this e-book.

Finally, we would like to thank our husbands and children for their support and encouragement.

Ruzanna binti Jubaidi
Norlela binti Zaman
Siti Aishah binti Ab Jalil

TABLE OF **CONTENTS**

CHAPTER 1 : OVERVIEW OF MANAGEMENT INFORMATION SYSTEM

By the end of the chapter student should be able to discuss:

- Overview of Information System
- Dimension of Information system

Introduction to Management Information System

This chapter aims to provide a comprehensive overview of information systems, explaining their fundamental concepts and historical development.

Information systems are integral to our daily lives, from personal computing to e-commerce to the strategic decision-making processes of global corporations.

In this chapter, we will look at the history of information systems, emphasizing their role in modern society as an essential component. This chapter also highlights the difference between Information Technology (IT) and Information Systems (IS). By understanding the history, uses, and distinctions between IT and IS, we can gain a more informed perspective on the present and future of information systems.

Information Technology (IT) versus Information System (IS)

In an organization, **information systems** provide data for decision-making and control by collecting, retrieving, processing, storing, and distributing information.. It is like a digital tool or machine that helps people store, organize, process, and access information.

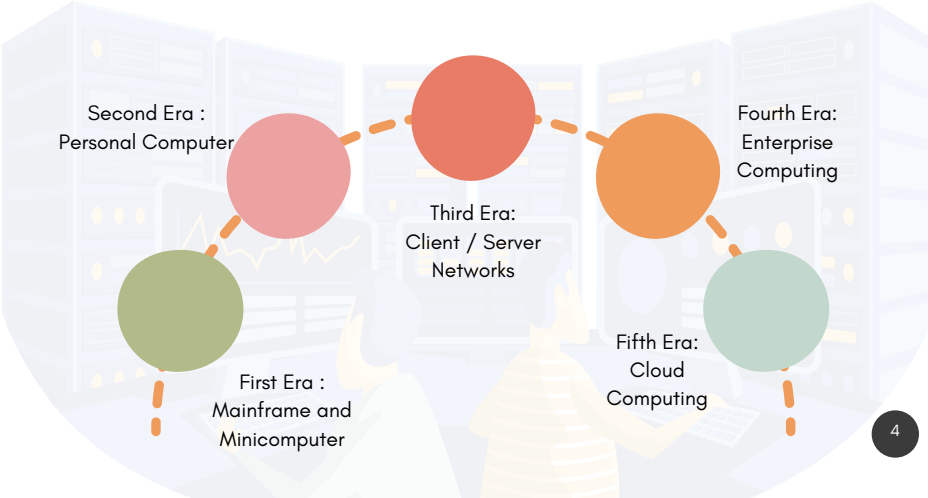
Think of it as a well-organized digital filing cabinet with a smart assistant. For example, consider an online bookstore like Amazon. It uses an information system to keep track of all the books it has in stock, their prices, and customer orders. When you search for a book on Amazon's website, that's like asking the digital assistant to find a book in the filing cabinet. The system quickly goes through its digital records, locates the book, and displays details like its title, author, price, and customer reviews. When you buy the book, the system processes your order, arranges for delivery, and updates its records to reflect that the book is now reserved for you. In this way, information systems help businesses and organizations manage their data efficiently, which makes it easier for you to find and buy things, among many other tasks in our digital world.

By contrast, **information technology (IT)** refers to all the hardware and software that is required for a business to meet its goals. A major function of information technology is to acquire, process, store, and disseminate digitized information or data. Additionally, it strives to improve technology's utilization to advance business goals. It is the magic behind the scenes that lets us do all sorts of cool stuff, like sending messages, streaming videos, and playing video games. Think of it as the engine that powers your digital devices.

Sending a text message to a friend is an example of using IT. Your words get turned into digital signals, travel through the air or cables, and then magically appear on your friend's phone as a message. It is as if you wrote a note, and it was instantly delivered by a friendly digital messenger. Furthermore, when you watch a video on YouTube, that is also thanks to IT – videos are transformed into digital code, sent over the internet, and then your device turns that code back into moving pictures and sound.

Information Systems History

The history of information systems is a fascinating journey through different technological generations. It begins with the mainframe era, where central computers dominated data processing. As we moved into the personal computer era, individuals gained access to computing power, transforming work and everyday life. The client/server era introduced a networked approach to data management, improving collaboration. The enterprise computing era facilitated inter-organizational data exchange, albeit with increased complexity. In today's era of cloud computing, information and applications reside in virtual environments, providing unprecedented accessibility and flexibility..



General Purpose Mainframe and Minicomputers Era : (1959 To Present)

Before 1965, computing was done on large mainframe computers in large, specially designed rooms. A temperature control system was installed in the room to ensure that the machines were continuously operating at their optimal levels.

Mainframes (1959 - Present)

Developed in the 1960s, the mainframe was the first computer to provide multitasking, time sharing, and virtual memory. With the ability to support thousands of remote terminals, this system is highly centralized and controlled by programmers and system operators.

Mainframe

Minicomputers (1959 - Present)

In comparison to mainframes, minicomputers are more cost-effective. Minicomputers make it possible to perform decentralized computing tailored to the specific needs of individual departments or business units instead of using a huge mainframe to share resources. This decentralization means that businesses can save money by not having to purchase and maintain a large mainframe, and they can also tailor their computing power to the specific needs of each department or business unit.

Personal Computer Era : (1981 To Present)

This era began in 1965 and was mainly due to the introduction of the microprocessor. Companies could now afford cheaper personal computers, which provided access to computing power that would have cost exorbitant money just one decade before.

By the 1980s, personal computers were becoming much more affordable; hence, they were made available to the mass market. The predominant ones then were the Apple I and the IBM personal computer, commonly called PC. The PC was friendlier to businesses, which explains why it rose to popularity in those early days.

Minicomputer

Personal Computer

Client / Server Era (1983 To Present)

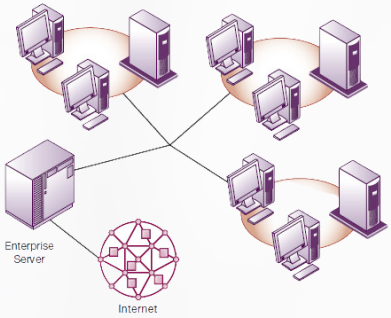
Compared to personal and mobile computers, server computers perform better. Within a network, they control access to resources such as input devices, output devices, storage devices, and data. Servers store centralized data and files within an organization. Users within the organization can also access this information through the intranet. Content and files are usually stored on a server connected to the Internet and meant for external users. It can be accessed by many users simultaneously, internally or externally.

Compared to a personal computer, a server is a bit bigger. It is usually stored in a locked room for security reasons because it contains a large amount of organizational data and information. Depending on the configuration, servers can cost as little as a few thousand ringgit up to many tens of thousands ringgit.

Server

Enterprise Computing Era : (1992 to Present)

Information can be shared freely within and between organizations through enterprise-wide networks. It includes public infrastructures such as the telephone network, the internet, and public network services, including mainframes, servers, personal computers, and mobile devices.



Cloud and Mobile Computing Era: (1992 to Present)

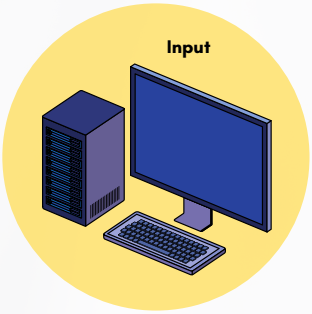
Client/server models proved to be very successful, but companies were faced with new challenges. Many large firms have had difficulty integrating their local area networks into a single, coherent corporate computing environment. It was difficult to communicate and share data between applications developed by different departments and divisions in a firm. With cloud and mobile computing, users have access to shared computing resources (computers, storage, applications, and services) over networks, most often the internet.

Cloud computing can be accessed from any connected device and location. Hundreds of thousands of computers are located in cloud data centres. Depending on the client machine, these computers can be accessed through desktop computers, laptop computers, tablets, entertainment centers, smart phones, and other internet-enabled devices.

BASIC ACTIVITIES IN INFORMATION SYSTEM

INPUT

- The input process involves capturing or collecting raw data from within or outside the organization.
- example: The system processes sales orders by verifying inventory availability, calculating totals, and updating inventory levels after a sale is completed.



Transaction Processing System Data

Other Data

Manaement Infomation System
System Programms

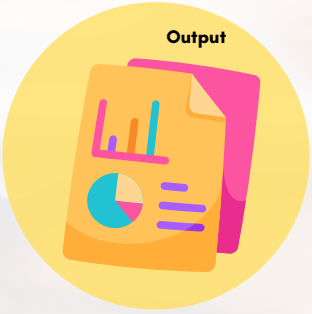
Summarization

PROCESSING

- Any data that has been entered into a computer system by activities include calculation, comparison, sorting, classifying and summarizing to produce meaningful output, this stage of processing converts raw data into a meaningful set of information for the end user.

OUTPUT

- Involves the data that have been produced by a transformation process the main goal of the output activity is to produce appropriate information for end users, includes messages, reports, forms, graphic images, video, audio responses, paper products or multimedia.
- Example: Reports on sales performance, revenue, and product trends are generated to help sales managers and executives make strategic decisions



Schedule reports

AdHoc Reports

COMPONENTS OF INFORMATION SYSTEM

1.HARDWARE

tangible component visible to the user.

Example: printer, scanner, monitor, keyboard, video screen

2. SOFTWARE

set of instructions to the computer hardware to perform a specific task. such as programs or applications. it is used for processing data and presenting it in a meaningful form to aid managerial decision-making. there are system software, application software, cloud, computing, and open sources software

3. DATA

raw fact represents events occurring in the organization and environment before they have been organized and arranged into a meaningful form. data creates value for an organization's resources. data can be created, stored, retrieved, manipulated, edited, processed, and analysed in multimedia format such as text, image, video, and audio. In a business transaction system, data is collected during the recording of transactions, processed, and analyzed later for decision-making.

4. PEOPLE

INFORMATION SYSTEM SPECALISTS

The development and operation of information systems is carried out by a group of people. These individuals range from Systems Analysts, Software Developers, Programmers, System Operators, Testers, Computer Operators to other Professionals involved in the management, technical, and clerical aspects of information systems.

END USERS

End users can also be referred to as clients or users. The individuals or groups who take part in the utilization of information systems or the outcomes they produce. Their roles can include accountants, salespeople, engineers, clerks, customers, or managers. Usually, they can be found at any level of an organization. As knowledge workers, they usually spend most of their time communicating and collaborating with teams and groups to generate, use, and distribute information.

5. PROCESS

a series of steps undertaken to achieve a desired outcome or goal. Process which involves a transformation process that converts input into output.

Input

- Processing data entered into the system by capturing and assembling them.
- Activities include data entry recording or editing.
- Example: Data on a sale transaction may be recorded using online order form. The data would then be entered into a computer system by sales personnel.

Processing

- Any data that has been entered into a computer system by activities include calculation, comparison, sorting, classifying and summarizing to produce meaningful output.
- This stage of processing converts raw data into a meaningful set of information for the end user
- Involves the data that have been produced by a transformation process

Output

- As part of the output activity, information is produced for the end users, such as messages, reports, forms, graphs, videos, audio, paper and multimedia products.
- Example: Data is processed to analyze sales trends, customer preferences, and the performance of products or sales representatives, helping to make informed marketing and sales decisions.

Feedback

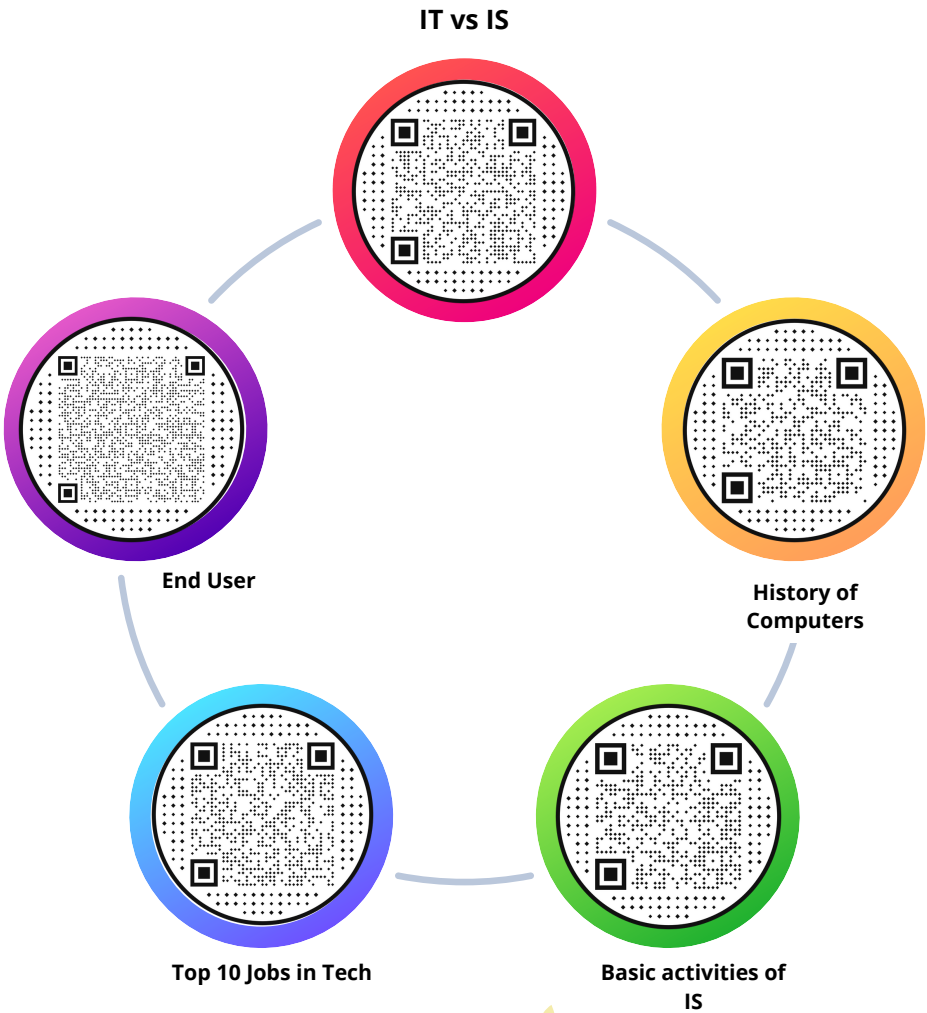
- Refers to response received on the performance of a system.
- Example: Data received on sales performances is feedback to a Sales Manager

Control

- As part of controlling, feedback is monitored and evaluated to determine if a system is achieving its goals.
- Example: Following feedback on a salesperson's performance, a Sales Manager reassigns them to new sales territories in order to enforce control.

Storage

- Data is retained in an organized manner for later use in processing and can also be retrieved by end users


IT vs IS
History of Computers
Basic activities of IS
Top 10 Jobs in Tech
End User

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

CHAPTER 2 : MANAGEMENT INFORMATION SYSTEMS BASIC: HARDWARE SOFTWARE AND NETWORKING

By the end of the chapter student should be able to explain:

- The computer hardware and software
- Types of network

MIS: Hardware Software and Networking Overview

Welcome to this exciting second chapter of your journey into technology. In an age when computers and networks are the lifeblood of our lives, understanding fundamental building blocks is crucial. This chapter aims to explore the world of computer hardware. Each category plays a unique role in shaping our digital interactions. As we delve deeper, you'll gain a newfound appreciation for how these physical elements work together harmoniously to perform the tasks that we often take for granted.

Our journey continues into software, where you'll uncover the distinction between system software and application software. These two categories are the yin and yang of computing, with system software serving as the backbone, while application software delivers the tools and programs that cater to our specific needs. As you navigate the complexity of this digital ecosystem, you'll understand not only how computers function but also how they adapt to serve our diverse purposes.

The final portion of this chapter will shine a spotlight on the vital networks that connect these computers. This will bring us closer together in a globally interconnected society. We'll discuss the various types of networks, from the localized efficiency of Local Area Networks (LANs) to the expansive reach of Wide Area Networks (WANs), and everything in between.

Definition of computer hardware

Computer hardware refers to the components that perform input, processing, storing, and exchanging data. Computer hardware can be classified into 4 types; (i) input devices, (ii) processing devices, (iii) output devices, as well as (iv) storage devices.

Classifications of computer hardware

Input devices gather data and convert them into electronic form for computer use. Keyboards, computer mouse, touch screens, optical character recognition, and digital scanners are examples of input devices

Input Device	Description
Keyboard	Text and numerical data are entered using this method.
Computer mouse	The handheld device enables users to control a cursor's position and select commands on a computer display screen by point-and-click. A trackball or touch pad is usually used on laptop computers instead of a mouse as a pointer.
Touch screen	A sensitized display screen that allows users to interact with computers by touching the surface. A multitouch device, such as an iPhone, iPad, and multitouch PC, is found in airport kiosks, retail stores, and restaurants.
Digital scanner	An image-to-digital converter that converts images (such as pictures) into digital files.
Optical character recognition	An electronic device that converts special characters, marks, and codes into digital forms. Optical codes are most commonly used as bar codes.
Pen-based input	Using an electronic stylus, handwriting is recognized digitally by devices that convert the motion into digital data.
Audio input	Designed to convert voices, music, or other sounds into digital form for computer processing.
Sensors	An environmental sensor that collects data directly from the environment for input into a computer. A farmer, for instance, can use sensors to monitor soil moisture.

Example of input device

Optical character recognition

Processing devices, an integral component of a computer system, plays a vital role in managing the storage and retrieval of information. By executing program instructions, these devices handle data processing tasks encompassing input-output activities, logical comparisons, and numerical computations.

Processing Device	Description
Central Processing Unit (CPU)	responsible for carrying out any instruction, ensures the coordination of all other computer units' operations, ensuring the smooth functioning of the system.
Graphics Processing Unit (GPU)	Gaming, video editing, and computational design require GPUs, which are specialized processors designed to handle complex graphics calculations.

Output devices display the processed data

Output Device	Description
Display	Monitors that have flat-panel (LCD) display screens or plasma screens
Printers	Devices that print hard copies of output information. There are two types of printers: impact (such as dot matrix printers) and nonimpact (such as laser, inkjet, and thermal transfer printers).
Audio output	Speakers, headphones, and ear buds are examples of audio devices that convert digital output data into intelligible speech, music, or other sounds.

Storage device, also known as storage medium, storage media, or digital storage, is a hardware component that enables the temporary or permanent storage of information. Its primary function is to hold, transfer, and retrieve data files, and it can be used internally or externally with a computer system, server, or similar computing devices.

Output Device	Description
Hard Disk Drive (HDD):	A hard disk drive is a common type of storage device used in computers and laptops. It consists of rotating magnetic disks that store data. The data is read and written using magnetic heads, providing non-volatile storage with relatively large capacities.
USB Flash Drive	USB flash drives, also known as thumb drives or pen drives, are portable storage devices that connect to computers through USB ports. They use flash memory to store data and are convenient for transferring and storing files. USB flash drives come in various capacities and are widely used for backup, file sharing, and carrying data on the go.
Optical Disc	Optical discs, such as CDs, DVDs, and Blu-ray discs, are storage devices that use laser technology to read and write data. They are commonly used for storing software, music, movies, and other multimedia content. Optical discs provide relatively large storage capacities, but they are not rewritable like magnetic or flash-based storage devices.

Definition of Computer Software

Computer software manages and coordinates the hardware components of an information system according to detailed instructions. Programs enable hardware to do a specific task. Software is used to run the computer.

Classifications of computer software

Software can be classified into 2 types:

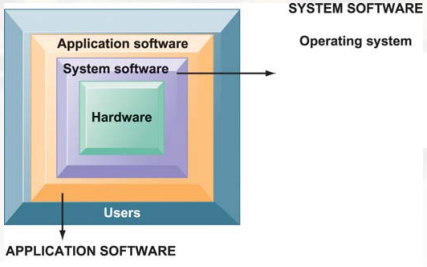
(i) System software manages the resources and activities of the computer. The system software surrounds and controls access to the hardware. The system software that manages and controls the computer's activities is called the operating system.

In a computer system, the operating system is the chief manager, allowing the system to handle multiple tasks and users simultaneously. User interactions with the computer are controlled by the operating system.

System software	Description
Windows 11	The latest Windows client operating system, which supports mobile devices, multitouch devices, and traditional PCs, as well as voice search.
macOS	Macintosh operating system that supports multitouch and is highly visual and user-friendly. MacOS Sonoma is the most recent version.
Linux	Open source, reliable alternative to UNIX and Windows operating systems that runs on many types of computer hardware and can be modified by software developers

(ii) Application software needs to communicate with system software in order to function. Business applications are developed using application software. A computer application is used to perform a particular task for a user, such as generating a mailing list or processing an order. Most system and application software nowadays is purchased rather than custom-programmed.

Software Tool	Capabilities	Example
Word processing	Various formatting options are available for changing documents electronically.	Microsoft Word
Spreadsheet	Data is organized into columns and rows. Whenever a user changes a value on a spreadsheet, all other related values are automatically updated.	Microsoft Excel
Desktop publishing	Creates professional-looking documents, brochures, or books	Adobe InDesign
Multimedia Software	Video, audio, and text edits can be performed with these software programs. It allows you to combine text, videos, audios, and images. Through multimedia software, photos, animations, graphics, and charts can be added to a text document.	VLC player, Window Media Player
Enterprise Software:	Business operations are supported by these software programs. Typically, it is used in large organizations with a large volume of business. In addition to accounting, billing, and order processing, it can also be used for other purposes.	CRM (Customer Relationship Management), BI (Business Intelligence)

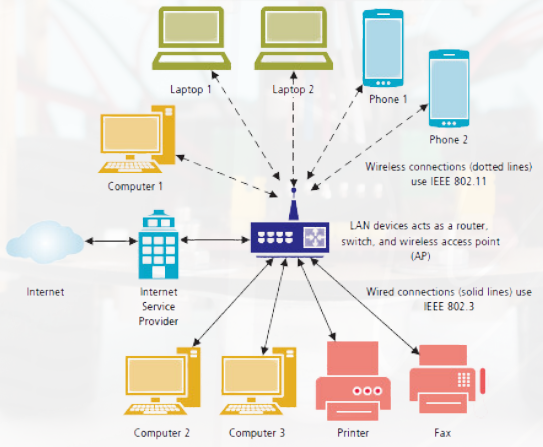


Application software is the primary tool used by end users. It is essential to design software specifically for a specific machine to ensure that it is compatible with it.

Types of network

Historically, firms used telephone networks and computer networks to communicate. Telecommunications regulations are being deregulated and information technology is advancing quickly, which is leading to the integration of Internet and telephone networks into one digital network. A computer network would be required if two or more employees in the same office needed to connect their computers. In essence, a network comprises connected computers.

In a **Local Area Network**, computers and other digital devices are connected within a radius of half a mile or 500 meters. There are several computers in a small office that are connected by LANs, or you can connect several computers in a building that are close by each other. LANs are fast and cost-effective. A network can have two to several hundred computers connected. A LAN is characterized by a single location. LANs rely on wired connections to increase speed and security, but wireless LANs (WLANs) can also be used.

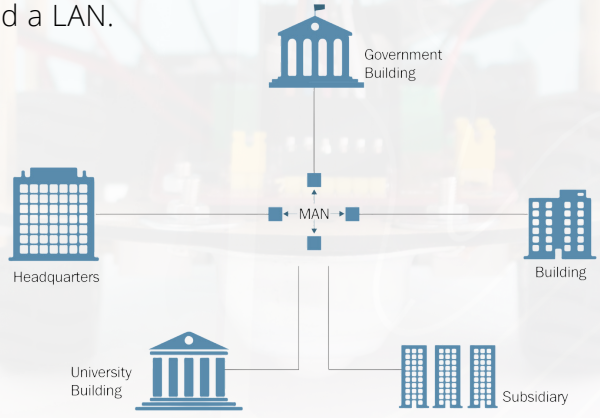


Local Area Network

A **campus area network (CAN)** usually forms a bigger network, designed for a campus environment. The coverage area can be up to 1,000 meters (a mile), if it is on a college campus or if it is on a corporate facility. CANs are designed to cover a large area, and the range is determined by the type of technology used. CANs use wireless technology, such as Wi-Fi, Bluetooth, or Ethernet, which allows them to be transmitted over long distances. CANs are also designed to be resilient to interference and to provide a reliable connection.

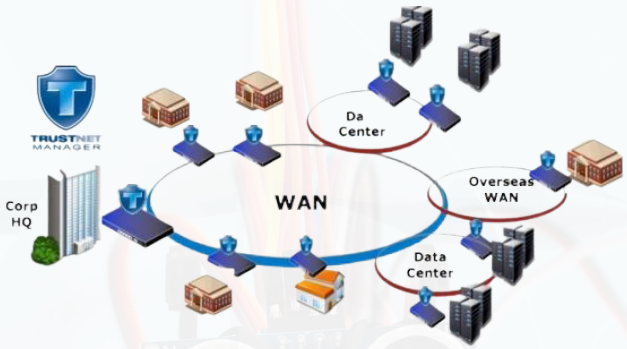
Campus Area Network

Metropolitan Area Network (MAN) is larger than LAN. It connects LANs across an entire city, campus or region. Depending on the configuration, a MAN can cover up to tens of miles. MANs are networks that span metropolitan areas, usually cities and their suburbs. Geographically, it lies between a WAN and a LAN.



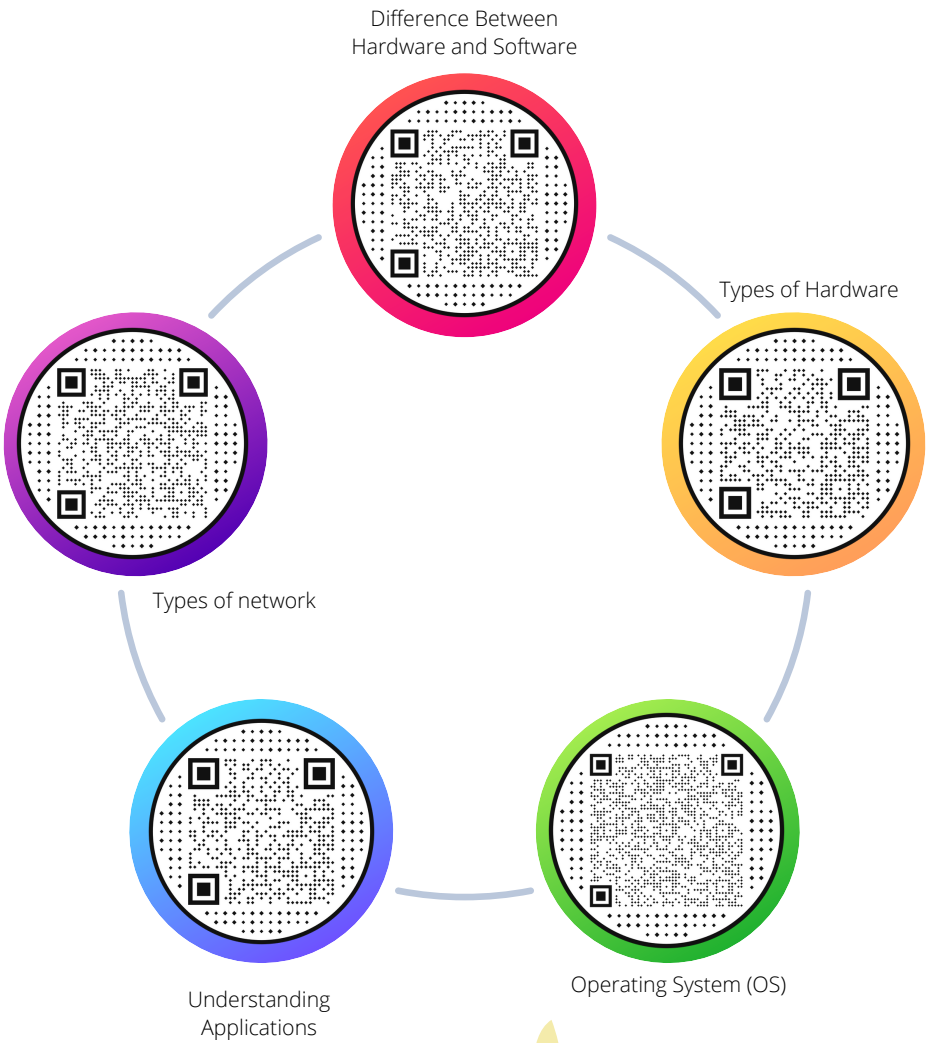
Metropolitan Area Network

Networks that serve large geographical areas, such as an entire country or the whole world, are known as **Wide Area Networks (WANs)**. There can be multiple smaller networks within a WAN, such as LANs and MANs. An example of a wide area network is the Internet.



Wide Area Networks

Type	Area
Local Area Network (LAN)	Up to 500 meters (half of mile), an office or Floor of a building
Campus Area Network (CAN)	Up to 1,000 meters (a mile), a college campus or corporate facility
Metropolitan Area Network (MAN)	A City or Metropolitan Area
Wide Area Network (WAN)	A transcontinental or global area


Difference Between
Hardware and Software
Types of Hardware
Operating System (OS)
Understanding
Applications
Types of network

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

CHAPTER 3 : INFORMATION SYSTEM SECURITY

By the end of the chapter student should be able to discuss:

- The threats to information security
- Information security

Introduction of Malicious Software

In our increasingly digital and interconnected world, the importance of information security cannot be overstated. This chapter aims to provide a entry point into safeguarding valuable data and systems from a spectrum of threats. Our first step will be to expose the various types of malware that can infiltrate and compromise our digital environments. We will also examine computer crimes, categorizing these unlawful operations that exploit digital vulnerabilities.

Continuing our journey, we will focus on the strategies and measures required to safeguard our information assets. We will elaborate on information security by exploring the vital controls that protect our information systems. These controls include mechanisms and policies to thwart unauthorized access and protect data integrity. Additionally, we will discuss information resource controls, emphasizing the importance of managing and securing digital and physical information assets.

Types of Malicious Software

Computer viruses, worms, Trojan horses and other malicious software programs are classified as malware.

Viruses are malicious programs that attach themselves to other programs or data files in order to execute without the user's knowledge or approval.

A computer virus usually carries a “payload.” The payload can be benign, like instructions to display a message or image, or highly destructive. It may cause a computer to run improperly, destroy programs or data, clog computer memory, reformat a computer's hard drive, or clog computer memory.

When humans send an e-mail attachment or copy an infected file, viruses spread from computer to computer.

A **worm**, which is an independent computer program that copies itself from one computer to another, is transmitted through a network. Unlike viruses, which depend on human behavior when spreading from computer to computer, worms can operate independently without attaching themselves to other computer files.

When a **Trojan horse** is launched, it appears to be benign, but then performs an unwanted action. Since Trojan horses do not replicate, they are not actually viruses, but they are often used by hackers to spread viruses.

Trojan horse is derived from the Trojan War, in which the Greeks used the Trojan horse, a huge wooden horse, to entice the Trojans to open their fortified city gates. As soon as the Greek soldiers entered the city walls, they revealed themselves and captured the city.

Types of Computer Crimes

A **hacker** is someone who attempts to access a computer system without authorization. The term "cracker" is commonly used in the hacking community to describe a hacker with criminal intentions, though the terms are often used interchangeably outside of the hacking community. Typically, hackers a gain access to Web sites and computer systems by exploiting vulnerabilities in the security protections employed by those sites and systems.

Additionally, **spoofing** can be accomplished by redirecting a Web link to a different address than the intended one, thereby misleading the recipient into believing they have reached the intended website. In the case of hackers redirecting visitors to a fake Web site that looks almost identical to the genuine one, they can then collect orders and process them, effectively stealing business and sensitive customer data from the genuine site.

Information traveling over a network is monitored by a **sniffer**, which is a type of eavesdropping software. When used for legitimate purposes, sniffers can provide valuable insight into network trouble spots or criminal activity, however, when used for criminal purposes, they can cause significant damage and are difficult to detect. By using sniffers, hackers are able to steal proprietary information from any part of a network, including e-mail messages, company data, and confidential documents.

An **identity theft** occurs when individuals or organizations have their personally identifiable information (PII) stolen and used without their consent by malicious actors. Among the sensitive data that can be stolen are names, credit card information, social security numbers and other personal information. An individual who commits identity theft may use this information for fraudulent purposes, such as making unauthorized purchases, accessing bank accounts, or committing other crimes on behalf of the victim. Assume that John uses his credit card to make online purchases and to conduct various financial transactions.

The term **Denial-of-Service (DoS)** refers to attacks designed to overwhelm networks, systems, and online services with excessive traffic. In a DoS attack, the goal is to make a service or system unavailable to its intended users, resulting in inconvenience, financial loss, or other disruption.

Consider a DoS attack on a major e-commerce website, "ShopNow.com," in which a malicious actor or a group of individuals floods ShopNow.com's web servers with a staggering number of HTTP requests, far beyond what the servers are capable of handling, using a botnet (a network of compromised computers). Due to the high traffic volume, the web servers become overloaded, consuming all CPU, memory, and bandwidth.

A legitimate user trying to make a purchase or browse products now finds the website extremely slow or unresponsive. Others may not be able to access the site at all, while others may receive error messages. ShopNow.com's operations are disrupted, resulting in financial losses, customer frustration, and reputational damage.

Click fraud occurs in online advertising, particularly in pay-per-click (PPC) advertisements. Online advertisements are repeatedly clicked on by individuals or automated bots with the aim of increasing advertising costs or depleting the advertising budgets of competitors. Advertisers can lose money due to click fraud, since they pay for every click on their ads, even if those clicks aren't valuable or genuine. Suppose your competitor sells a similar product and decides to commit click fraud to hurt your business. Your ad is repeatedly clicked on throughout the day by automated click bots or by individuals. In click fraud, your advertising costs are artificially inflated and you cannot reach legitimate customers.

An act of **cyberterrorism** involves using computer technology, networks, and the internet to commit a terrorist act. Cyberterrorism aims to create fear, disrupt critical infrastructure, and harm individuals, organizations, or nations. There are many essential services targeted by cyberterrorists, including power grids, financial systems, and government networks. Economic and social consequences can result from these attacks.

As part of military conflicts and warfare, **cyberwarfare** uses digital means, such as hacking, electronic warfare, and online attacks. A cyberwarfare operation can have a number of objectives, ranging from gathering intelligence to disabling or destroying critical infrastructure. Cyberwarfare activities are often conducted by nations and state-sponsored organizations, which can have far-reaching implications for national security.

Information Systems Controls

The development, safety, and application of computer programs are governed by **general controls** in the organization's information technology infrastructure. All computerized applications are controlled by a combination of hardware, software, and manual procedures.

A general control can be categorized into software, hardware, computer operations, data security, and processes for implementing system processes. Listed below are the functions of each control.

TYPES OF GENERAL CONTROL	DESCRIPTION
Software controls	Maintain a record of software programs, system software, and computer programs being used by unauthorized people, and prevent unauthorized access and use.
Hardware controls	Make sure the computer hardware is physically secure and that there are no malfunctions. In order to maintain constant service, critical organizations also need to ensure their computers are backed up or run continuously.
Computer Operation controls	Maintain a consistent and accurate oversight of the computer department's work. Additionally, a backup and recovery strategy for abnormally ending processing is included, along with control over the setup of computer processing jobs.
Data security controls	While they are in use or in storage, make sure that valuable business data files are protected against unauthorized access, change, or destruction.
Implementation controls	In order to ensure proper control and management of the systems development process, audit the process at various points of the development process.
Administrative controls	Incorporate standards, rules, procedures, and control disciplines into organizational policies and procedures for the proper execution and enforcement of general and application controls.and application controls are properly executed and enforced.

An **application control** refers to a specific control that is specific to an application, such as the payroll program or an order processing system.

This application keeps only authorized data completely and accurately processed using automated and manual procedures. Controls for applications can be categorized as input, processing, and output controls.

TYPES OF APPLICATION CONTROL	DESCRIPTION
Input controls	Ensure that data entered into the system is accurate and complete. A number of input controls are available for approving input, converting data, editing data, and handling errors.
Processing controls	As part of the processing control, it ensures that data are complete and accurate during updating.
Output controls	By keeping output control in place, computer processing results are accurate, complete, and well-distributed.

Information Resources Controls

a. Authentication

A person's ability to verify that they are who they claim to be. Access to a system requires authentication and authorization. You can use a password, a token, a smart card, or a biometric security token.

i. Password

- Authentication is often established by using password known only to authorize users.
- User uses a password to log on to a computer system and may also use passwords for accessing specific systems and files.
- Users often forget passwords, share them or choose poor passwords that are easy to guess, which compromises security.
- Passwords can also be “sniffed” if transmitted over a network or stolen through social engineering.

ii. A smart Card

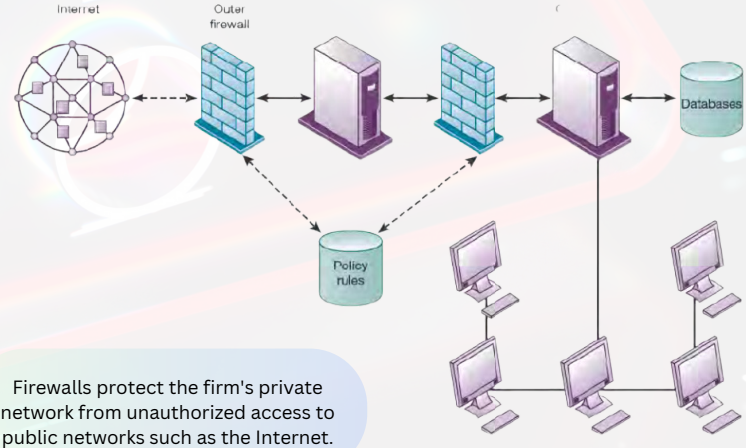
- A smart card contains a chip formatted with permissions and other data about the size of a credit card.
- Associated with electronic payments.
- An access card reader interprets the data contained on a smart card and grants access.

iii. Biometric Authentication

- Uses systems that read and interpret individual human traits, such as fingerprints, irises, faces, retinal images and voices, in order to access.

b. Firewalls

- In a firewall, unauthorized users are prevented from accessing private networks. A system that allows inbound and outbound network traffic to be controlled using a combination of hardware and software. An internal network firewall is typically placed between the organization's internal network and an external network, such as the Internet, that is distrusted by the organization. It is used to protect one part of a company's network from the rest of the network.
- The firewall acts as a gatekeeper, verifying each user's credentials before granting access. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. The system checks this information against the access rules programmed by the network administrator. A firewall prevents unauthorized access to the network.



Firewalls protect the firm's private network from unauthorized access to public networks such as the Internet.

c. Intrusion Detection System (IDS)

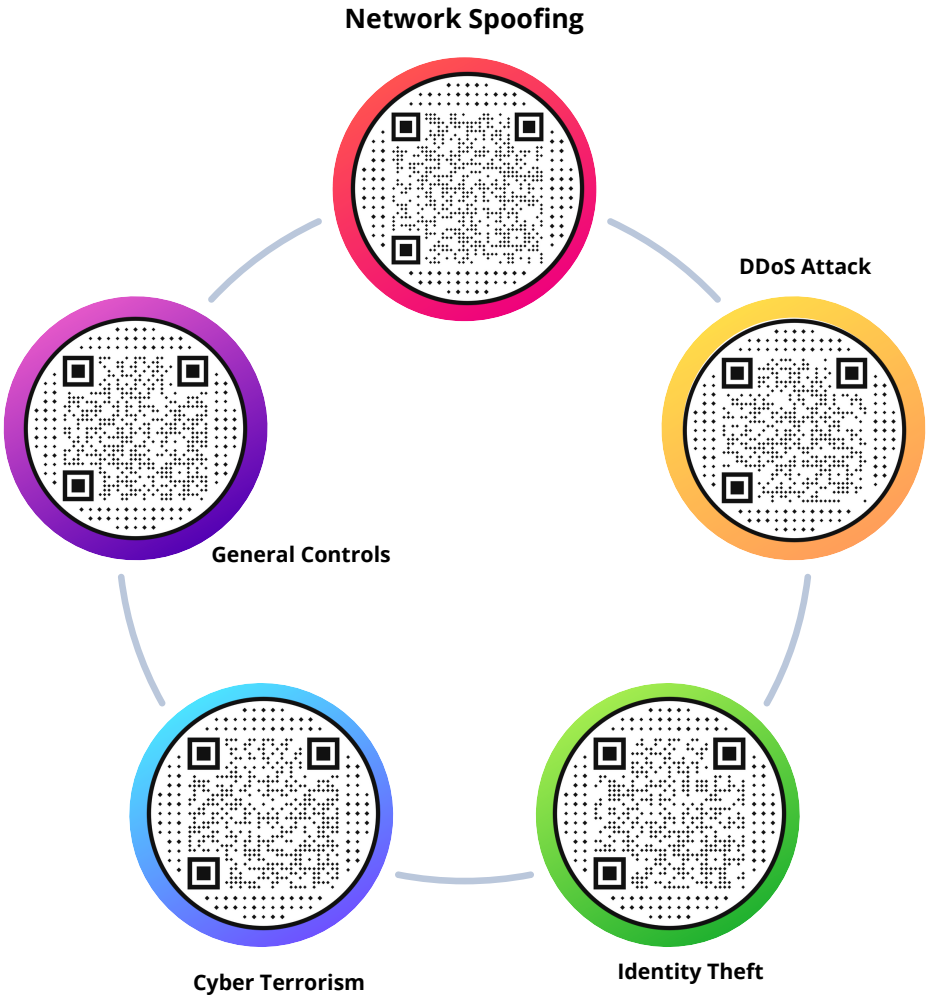
- Prevent unauthorized access to files and databases by blocking suspicious network traffic.
- Detecting intruders at the most vulnerable points or "hot spots" of corporate networks using full-time monitoring tools
- In the event of a suspicious event, the system generates an alarm. In scanning software, patterns are identified that indicate known methods of computer attack, such as bad passwords, and messages are sent alerting the user if a file has been modified or removed.
- Security attacks are detected by monitoring software as they occur.
- If unauthorized traffic is detected on a network, IDS can be customized to shut down the sensitive parts..

d. Antivirus and Antispyware Software

- Antivirus software prevents, detects and removes malware, including computer viruses, computer worms, Trojan horses, spyware and adware. Most antivirus software is effective only against malware already known when the software was written.
- To remain effective, the antivirus software must be continually updated.

e. Unified Threat Management System (UTMS)

- A combination into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, Web content filtering and antispam software.
- Help businesses reduce costs and improve manageability. Available for all sizes of networks, initially aimed at small and medium-sized businesses.
- Example: Crossbeam, Fortinet and Check Point.


Network Spoofing
DDoS Attack
General Controls
Cyber Terrorism
Identity Theft

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

CHAPTER 4 : INFORMATION SYSTEMS AND ORGANIZATION STRATEGY

By the end of the chapter student should be able to explain:

- The concepts of management information system in business
- The development and implementation of information system in modern organizations .
- Ethical and legal implication of Information System in current business issues

Introduction of Information Systems and Organization Strategy

Information systems are the backbone of modern organizations, and understanding their diverse types and functions is crucial in the digital age. This chapter aims to provide an understanding of various information systems and how each plays a vital role in the complex information ecosystem.

Nevertheless, information systems are not isolated; they are shaped, developed, and used by a wide range of people from a variety of backgrounds. This chapter also focuses on the pivotal roles people play in designing, developing, and utilising these systems. From the programmers who create them to the end-users who rely on them for their daily tasks, the human aspect of information systems is just as vital as the technology itself. Furthermore, we will explore into the different types of users, from knowledge workers to operational staff, who interact with these systems. Each user has unique needs and demands. By the end of this chapter, you will have a firm grasp of the dynamic world of information systems and the people who drive their success.

Types of Information System

Office Information System | Transaction Processing System | Management Information System | Decision Support System | Executive Support System

Office Information System(OIS)

An Office Information System (OIS) is a type of information system designed to support and facilitate day-to-day operations and tasks within an office or workplace. Using OIS, employees can efficiently and easily manage, process, and share their information. The system consists of various software applications and hardware components tailored to meet specific office-related requirements.

The purpose of an OIS is to improve productivity and streamline office operations by incorporating various functionalities, such as document management, communication, scheduling, and data storage.

TYPES OF OIS	DESCRIPTION
Word Processing Software	Maintain a record of software programs, system software, and computer programs being used by unauthorized people, and prevent unauthorized access and use.
Spreadsheet Software	Make sure the computer hardware is physically secure and that there are no malfunctions. In order to maintain constant service, critical organizations also need to ensure their computers are backed up or run continuously.
Email and Communication Tools	Maintain a consistent and accurate oversight of the computer department's work. Additionally, a backup and recovery strategy for abnormally ending processing is included, along with control over the setup of computer processing jobs.
Document Management Systems	While they are in use or in storage, make sure that valuable business data files are protected against unauthorized access, change, or destruction.
Calendar and Scheduling Software	In order to ensure proper control and management of the systems development process, audit the process at various points of the development process.

Transaction Processing System (TPS)

The **Transaction Processing System (TPS)** automates and supports day-to-day business processes such as recording, processing, and managing day-to-day business transactions.

Organizations undergoing a high volume of routine transactions need TPS to process them efficiently and accurately. Transactions such as sales, purchases, payroll processing, and inventory management can be included in this category. Transaction processing systems are designed to ensure that transactions are processed in a timely, reliable, and consistent manner.

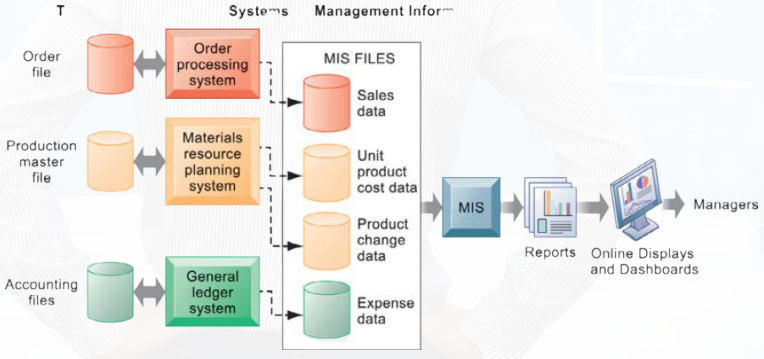
Components of TPS	Description
Data Entry	Transaction data is generally captured via point-of-sale terminals, barcode scanners, and employee entry.
Data Processing	TPS validates, records, and updates data in databases or other storage systems. Calculations, data transformations, and data integrity checks may be involved.
Real-Time Processing	Many TPS systems use real-time processing to ensure that transactions are recorded immediately and reflected in the system's databases instantly.
Data Management	TPS relies on databases for storing and retrieving transaction data. A database is designed to handle a large number of records efficiently and ensure data integrity
Reporting	TPS can be used to retrieve transaction data for analysis and reporting.

Management Information System (MIS)

In an organization, a Management Information System (MIS) collects, processes, stores, and distributes information to support decision-making and management functions. MIS enables managers at various levels to plan, control, and make informed decisions based on data, reports, and tools. The organization gains access to timely and relevant information that helps them achieve their goals

Components of MIS	Description
Data Collection	The MIS collects data from a variety of sources, including transaction processing systems, databases, and external sources.
Data Processing	This process involves sorting, aggregating, and calculating raw data into meaningful information.
Data Storage	MIS stores information in a structured manner, typically in databases, making it easily accessible
Information Retrieval	Reports and queries can be generated by managers using query and reporting tools
Information Presentation	MIS presents information in an understandable format, typically through reports, charts, and graphs.

For example, a report may be generated in the sales and marketing department showing that a particular product is selling well in a specific region. Once the target region has been identified, the marketing team can begin promoting the product.

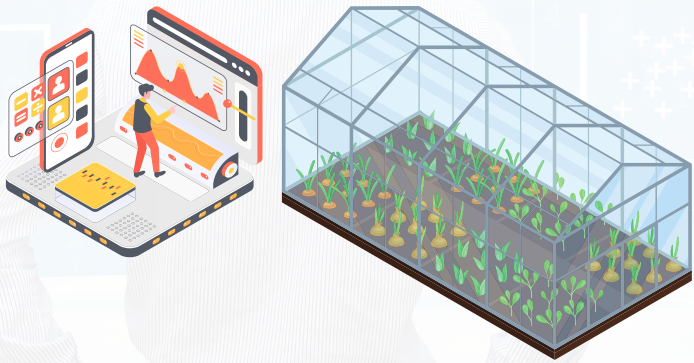


Decision Support System(DSS)

DSSs are information systems that help decision-makers, generally managers and executives, make informed and data-driven decisions. By providing tools and data, DSS enables complex problems to be analyzed and various options to be evaluated. In order to support decision-making, it combines information from different sources, analyzes the results, and presents them.

These tools enable users to quickly identify and analyze data, as well as to make decisions based on that data. As well as providing insight into potential risks and opportunities, DSS is also capable of predicting future trends.

Decision support systems are used by industries around the world on a daily basis. Farmers use DSS to determine when to plant, fertilize, and harvest their crops. Using analytics and decision support, Bayer Crop Science created "virtual factories" to analyze "what-if" scenarios at its corn manufacturing plants.

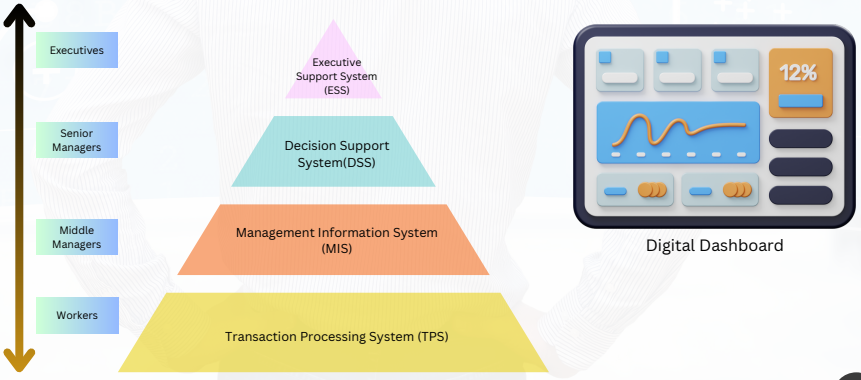


Executive Support System (ESS)

Executive Support System (ESS) combines many features of both MIS and DSS. These systems provide quick and easy access to information about an organization's performance for top executives.

Unlike in other situations, there is no agreed-upon method for reaching a decision. This requires judgment, evaluation, and insight. With an ESS, the CEO can monitor the firm's financial performance on a minute-to-minute basis based on working capital, receivables, payables, cash flow, and inventory, making decisions that affect the whole organization. A digital dashboard presents the information provided by ESS.

Components of ESS	Description
Strategic Performance Monitoring	Company executives can monitor the business's strategic performance in real time through the ESS. Key performance indicators (KPIs) measure revenue, market share, profitability, and customer satisfaction.
Market Analysis	Data sources included in the ESS include economic forecasts, competitor analysis, and industry reports. Market trends and competitor activities are summarized for executives.
Financial Dashboard	Financial dashboards with interactive charts and graphs are included. Monitoring financial performance and assessing revenue impacts of currency exchange rates is possible for executives.
Scenario Planning	The ESS is used by executives to analyze scenarios. By modeling new market entry, launching a new product line, and adjusting pricing strategies, they can predict potential outcomes. Analysis and projections are generated by the system.



People in Information Systems

People in Information Systems play a crucial role as technology and data management evolve. As experts in this field, they are at the forefront of designing, developing, and maintaining the systems that drive businesses and organizations forward. Whether system analysts, database administrators, software engineers, or cybersecurity specialists, people in Information Systems are the architects of the digital age, ensuring that data flows efficiently and securely and transforms into valuable insights that shape our modern world.

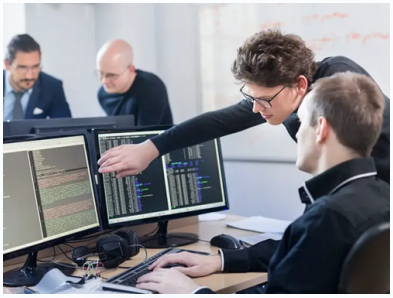
Roles of people in the Design, Development and use of Information systems

Programmers is a highly trained technical specialist who writes computer programs. Computers can perform specific tasks thanks to their programs. Besides developing programs, programmers must also troubleshoot, debug, and maintain them. Effective communication with nontechnical personnel is also essential.

The **System Analyst** is the primary liaison between the information systems groups and the rest of the organization. Systems Analysts translate business problems and requirements into information requirements and systems.

The System Analyst is the primary liaison between the information systems groups and the rest of the organization. Systems Analysts translate business problems and requirements into information requirements and systems.

Information Systems Managers coordinate the efforts of Programmers and Analysts, Project Managers, Physical Facility Managers, Telecommunication Managers, or Database Specialists. Additionally, they supervise computer operations and data entry staff.



A wide range of **external specialists** are involved in the day-to-day operations and long-term planning of an information system, including hardware manufacturers, software firms, and consultants.

A **Chief Information Officer (CIO)** is a senior manager who oversees the use of information technology within a company. An effective CIO should have a strong background in business, as well as information systems expertise, and play an active role in integrating technology into the firm's business strategy. Several large companies today have positions for Chief Security Officers, Chief Knowledge Officers, and Chief Privacy Officers, who work closely with the Chief Information Officer

The Chief Security Officer (CSO) is in charge of information systems security for the firm and is responsible for enforcing the firm's information security policy. Sometimes this position is called the Chief Information Security Officer (CISO) where information systems security is separated from physical security. The CSO is responsible for educating and training users and information systems specialists about security, keeping management aware of security threats and breakdowns and maintaining the tools and policies chosen to implement security

It has become so important to safeguard personal data and secure information systems that large corporations have established positions to do so. Data privacy laws are enforced by the **Chief Privacy Officer (CPO).**

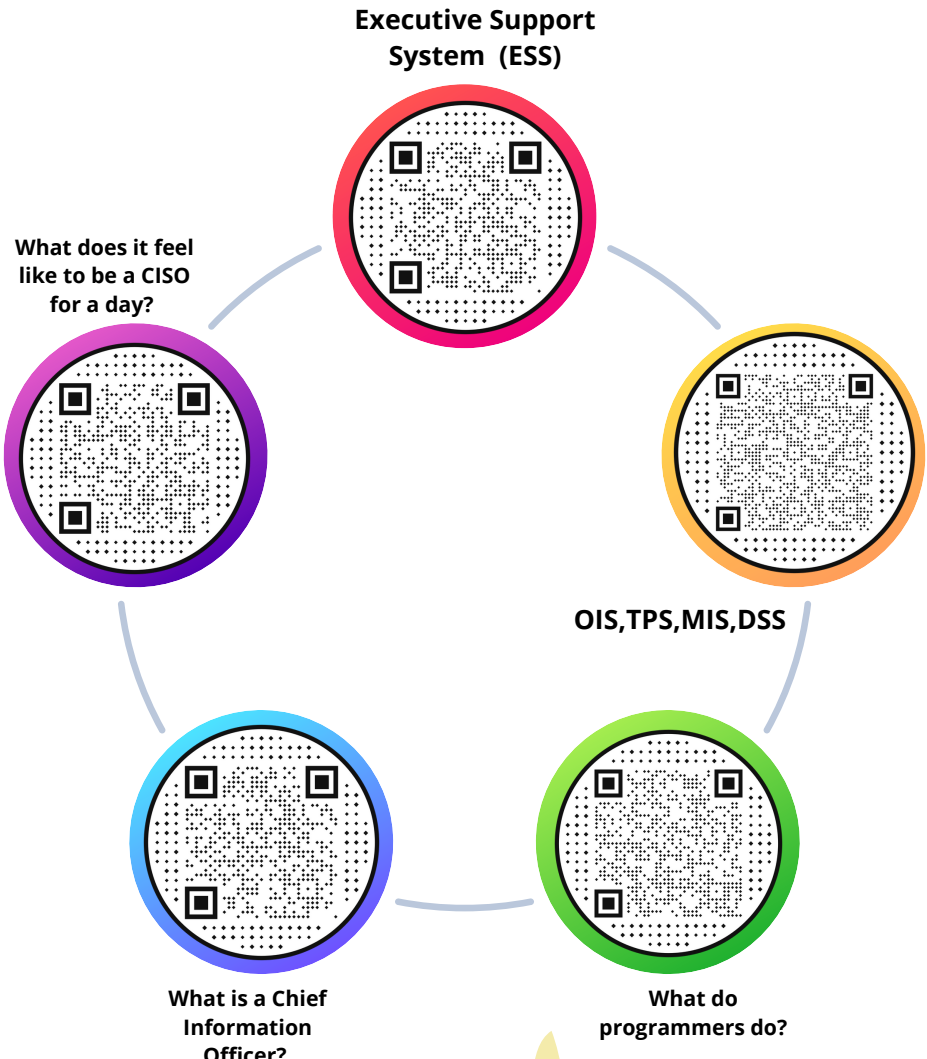
Chief Knowledge Officer (CKO) responsible for the firm's knowledge management program. The CKO helps design programs and systems to find new sources of knowledge or to make better use of existing knowledge in organizational and management processes

Chief data officer (CDO) is responsible for enterprise-wide governance and utilization of information to maximize the value the organization can real-ize from its data. The CDO ensures that the firm is collecting the appropriate data to serve its needs, deploying appropriate technologies for analyzing the data, and using the results to support business decisions. This position arose to deal with the very large amounts of data organizations are now generating and collecting

The term **end user** refers to a person or group of individuals who interact directly with or use information technology (IT) systems, software applications, or databases to fulfill specific goals, access information, or perform tasks.Users are ultimately responsible for consuming information provided by the system and are not required to be IT experts or system administrators.

Type of Users of Information Systems

LEVEL	ROLE	POSITION
Strategic Top-Level Managers	Implement organizational goals, policies, and strategies to achieve the firm's objectives.	Among the chief executives, presidents, vice presidents, and corporate heads are the chief executive, chief financial, chief operational and chief information officers.
Tactical Middle-Level Managers	In charge of implementing the goals set by the top managers.	Managers at all levels, including general managers, plant managers, regional managers, and divisional managers.
Operational First Level Managers	Their organizations require them to manage their work units on a daily basis	Office Manager, Line Manager, Department Manager, Supervisor and Store Manager


Executive Support System (ESS)
What does it feel like to be a CISO for a day?
OIS,TPS,MIS,DSS
What is a Chief Information Officer?
What do programmers do?

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

CHAPTER 5 : BUSINESS INTELLIGENCE

By the end of the chapter student should be able to explain:

- Business Intelligence
- Importance of Business Intelligence
- and apply Basic of Enterprise Reporting

Business Intelligence

As data becomes the new currency of business, Business Intelligence (BI) plays a key role in helping organizations maximize its potential. This chapter aims to provide an overview of business intelligence, exploring its essence and significance in today's business world. A key part of BI, Enterprise Reporting, allows organizations to generate, share, and analyze reports.

Business intelligence (BI) refers to the procedural and technical infrastructure that collects, stores, and analyzes the data produced by a company's activities. BI is a broad term that encompasses data mining, process analysis, performance benchmarking, and descriptive analytics.

BI has an array of tools for obtaining useful information from all the different types of data used by businesses today, including semi-structured and unstructured big data in vast quantities. These capabilities include data warehouses and data marts, Hadoop, in-memory computing, and analytical platforms. Some of these capabilities are available as cloud services.

Importance of Business Intelligence

- Improve ROI by understanding the business and intelligently allocating resources to meet strategic objectives.
- Unravel customer behavior, preferences and trends, and use the insights to better target prospects or tailor products to changing market needs.
- Monitor business operations and fix or make improvements on an ongoing basis, fueled by data insights.
- Improve supply chain management by monitoring activity up and down the line and communicating results with partners and suppliers.

Dashboard in report and presentation

Dashboards are typically used to compare data sets, charts, topics, and more, while reports usually cover specific topics. A report provides more detailed information about the performance of the system and is typically longer and more thorough than a dashboard.

Business Need Dashboard

The Business Need Dashboard provides a visual representation of an organization's specific business needs, objectives, and key performance indicators (KPIs). The dashboard is designed to assist decision-makers, business analysts, and other stakeholders in understanding and tracking the organization's goals and requirements.

Components of BND	Description
Customization	Company executives can monitor the business's strategic performance in real time through the ESS. Key performance indicators (KPIs) measure revenue, market share, profitability, and customer satisfaction.
Visualization	Data sources included in the ESS include economic forecasts, competitor analysis, and industry reports. Market trends and competitor activities are summarized for executives.
Real-Time or Periodic Updates	Financial dashboards with interactive charts and graphs are included. Monitoring financial performance and assessing revenue impacts of currency exchange rates is possible for executives.
Data Integration	It provides a comprehensive view of the business by integrating data from a variety of sources, both internal and external. The data may be gathered from CRM software, financial software, marketing platforms, and other sources.
Goal Tracking	Monitor progress towards specific business objectives and goals by using Business Need Dashboards. Targets can be set and actual performance can be compared.

Types of Dashboards

1. Enterprise Performance Dashboard

Enterprise Performance Dashboards are used by organizations to monitor and measure their overall performance and key performance indicators (KPIs) across various aspects of their business. It enables executives and managers to make informed decisions and align strategies with goals by providing a holistic view of the organization's performance. Using an enterprise performance dashboard, you can easily analyze data from multiple sources, departments, and systems in a single visual interface.

Example	Description
Revenue	The dashboard shows both current and historical revenue figures for the company. The current revenue is compared to the monthly and yearly targets.
Operational efficiency	A dashboard visualizes inventory levels and alerts you when they fall below a certain level.
Market Share Growth	A dashboard displays the company's market share growth over time compared to its competitors.

2. Customer Support Dashboard

Organizations use **customer support dashboards** to manage and monitor customer service operations. The solution provides a real-time, centralized view of key customer support metrics and performance indicators so customer service teams and management can improve customer service, response times, and issue resolution. Organizations deliver a superior customer experience with a dashboard as part of customer relationship management (CRM).

The following examples illustrate Customer Support Dashboards:

Example	Description
Ticket Volume	Using the dashboard, you can see the number of support tickets received each day in real time. Additionally, it provides an average for each month.
Timing of response	Color-coded heat maps show response times for different channels. Users can conduct an in-depth analysis of response time trends.
Time taken for resolution	In the dashboard, a line chart shows the average time taken to resolve support tickets.
The customer's satisfaction	Support managers can track overall customer satisfaction levels based on the scores displayed. It is possible to analyze feedback comments from customers.
Agent Workload	The user can see each agent's current workload, including the number of tickets open and their status.
Case Management	Customer support agents can access their open support cases directly from the dashboard, assign tickets to themselves or other agents, and update case details.

Using the Customer Support Dashboard, the software company can manage its customer support operations more efficiently. Ultimately, it improves customer satisfaction and enhances the quality of customer support by allowing managers to monitor key metrics, track agent performance, and respond to customer issues promptly.

3. Divisional Dashboard

In an organization, a Divisional Dashboard is used to monitor and assess the performance of specific departments or divisions. Using these dashboards, managers and stakeholders can see key performance indicators (KPIs) and metrics relevant to a particular business unit, facilitating informed decision-making and tracking progress towards departmental objectives.

The following is an example of a dashboard for a division:

Example	Description
Dashboard for the Sales Division	The dashboard displays real-time sales revenue data, compares it to targets, and provides historical data
Sales by Region	With the help of a map visualization, the sales division can identify high-performing and underperforming geographic regions
Marketing Division Dashboard	Key marketing campaign metrics are tracked in the dashboard, including click through rates, conversion rates, and return on investment (ROI)
Social Media Engagement	Marketing managers can assess their online presence by viewing bar graphs that depict engagement metrics from their social media channels.
Inventory Levels	Dashboards display real-time inventory data for various products, indicating stock outs, overstocks, and reorder points

The dashboards used by each division allow data-driven decisions to be made. Inventory managers can optimize stock levels and supplier relationships, while sales managers can focus on sales revenue. A Divisional Dashboard allows division-specific improvements and goal achievement while providing a segmented view of an organization's performance.

Creating Dashboard

Creating a dashboard reporting in a class allows for a more comprehensive and detailed approach. Here's a step-by-step guide for building a dashboard over this extended timeframe:

Step 1: Define Objectives and Data Requirements
Begin by clearly defining the objectives of your dashboard. Identify the key performance indicators (KPIs) and data sources required to achieve those objectives.

Step 2: Data Collection and Preparation
Gather the necessary data from various sources, ensuring it's clean, organized, and relevant. Perform data cleaning, transformation, and any necessary data integration.

Step 3: Select Dashboard Software
Choose a suitable dashboard creation tool or software, such as Tableau, Power BI, Google Data Studio, or Excel. Make sure participants have access to and are familiar with the chosen platform.

Step 4: Dashboard Planning and Design
Plan the layout and structure of your dashboard. Create a rough sketch or wireframe of the dashboard's visual arrangement.

Step 5: Data Visualization and Chart Creation
Input your cleaned data into the dashboard software. Build data visualizations, including charts, graphs, tables, and maps. Customize these visualizations to effectively convey your data insights.

Step 6: Interactivity and User Controls
Add interactive elements such as filters, slicers, and drop-down menus to allow users to explore the data. Ensure that the dashboard elements are well-connected and responsive to user inputs

Step 7: Styling and Branding
Customize the dashboard's appearance, including colors, fonts, and branding elements to make it visually appealing and consistent with your organization's identity.

Step 8: Testing and Optimization
Carefully review the dashboard for accuracy and functionality. Test user interactions, ensuring they work as intended. Optimize the performance and layout based on feedback and usability testing.

Step 9: Presentation and User Training
Present the completed dashboard to the class. Provide an overview of its features and functionalities. Offer training on how to use the dashboard effectively for monitoring and analysis.

Step 10: Feedback and Refinement
Encourage feedback and questions from participants. Discuss possible improvements and refinements based on user suggestions.

Step 11: Distribution and Implementation
Share the dashboard with participants, and provide instructions for accessing it.

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

CHAPTER 6 : ETHICAL AND SOCIAL ISSUES IN INFORMATION SYSTEM

By the end of the chapter student should be able to explain:

- Five moral dimension of information age
- Ethical and legal implications of information systems
- The privacy and data protection law in Malaysia

Introduction to Ethical and Social Issues in Information System

This chapter aims to explore five moral dimensions specific to the Information Age, examine into the ethical and legal implications of information systems, and gain a comprehensive understanding of privacy and data protection laws, with a focus on Malaysia's unique regulatory landscape. By acquiring this knowledge, students will be well-equipped to make informed decisions and contribute positively to the responsible use of information technology in today's society.

A person's moral behavior is guided by principles of right and wrong which are known as **ethics**. As information systems create opportunities for intense social change, they raise new ethical questions for both individuals and societies since they threaten existing power, money, rights, and obligations distributions.

The use of information technology can contribute to social progress, as did steam engines, electricity, and telephones, but it can also threaten cherished social values and lead to crimes. Information technology will lead to benefits for some and costs for others. We live in a society where ethical, social, and political issues are closely intertwined. The ethical dilemmas managers of information systems face are usually reflected in social and political discourse.

Five moral dimension of information age

Information, technology, and their use are a set of ethical considerations that comprise the moral dimensions of the information age. Several dimensions are involved, including information rights and obligations, property rights and obligations, accountability and control, systems quality, and quality of life. In order to better understand these dimensions, we'll look at examples from each:

1. Information Rights and Obligations:

   Individuals have the right to control how their personal information is collected, used, and shared. Individuals and organizations are ethically obligated to respect and protect these rights.
   As an example, some online tracking practices collect information without the individual's consent, which raises privacy concerns.

2. Property rights and obligations

   As the information age advances, intellectual property rights become increasingly important. Inventors and creators have the right to protect their work, and others are bound to respect that right.
   Infringing upon intellectual property rights can be found in online piracy, where copyrighted content is illegally shared and downloaded.

3. Accountability and control

   Organizations and individuals are responsible for their actions and decisions in the digital world. They should be held responsible for the consequences of their choices.
   For example, to ensure a safe online environment, social media platforms should moderate content and prevent the spread of hate speech and misinformation.

4. System quality

To maintain the integrity of information systems, quality, reliability, and security must be assured. Organizations must develop and maintain systems which meet high-quality standards.
For instance, software or hardware vulnerabilities that lead to data breaches or system failures raise ethical concerns regarding system quality.

5. Quality of life

Digital inclusion refers to ensuring that the benefits of the information age are accessible to all, thus minimizing the digital divide. By integrating digital technology into everyday life, all individuals can enhance their quality of life.

Providing affordable and reliable internet access can help close the digital divide and improve the quality of life in poor or underserved communities.

Every decision and action taken by individuals, organizations, and governments in the information age requires an ethical perspective that takes society, individuals, and the environment into account. As technology advances and the digital age looms, ethical considerations are essential for navigating the complexities and challenges it presents

Ethical and legal implications of information systems

There has been a growing number of ethical dilemmas resulting from the use of information systems in which one interest set is pitted against another. Some companies use voice recognition software to reduce the number of customer service representatives by allowing computers to recognize the responses of customers to a series of computer-assisted questions.

Basic concepts of ethics in information systems

a. Responsibility

Ethics requires a sense of responsibility. Taking responsibility for your actions means accepting the costs, duties, and responsibilities that may result from your actions.

Responsibility in information systems means acknowledging the potential consequences of one's decisions. The loss of sensitive customer data that results from data breaches is one example of an organization's responsibility. In Malaysia, an example of this occurred in 2017, when millions of customer records were exposed due to a data breach at a telecommunications company. After accepting responsibility, notifying the affected individuals, and taking steps to rectify the situation, the company was required to take appropriate action.

b. Accountability

Accountability means that individuals and organizations are answerable for their actions and decisions. It involves taking responsibility for the outcomes of those actions and being able to explain and justify them. A chief information officer (CIO) is accountable for the organization's information systems. If a critical system failure occurs, the CIO is accountable for ensuring that proper safeguards were in place, that adequate redundancy was implemented, and that incident response plans were followed.

c. Liability

Liability involves assigning responsibility for actions and their consequences. In information systems, it includes determining who is responsible when things go wrong or when data breaches occur. If a healthcare provider's electronic health records system experiences a security breach, resulting in the exposure of patient data, the organization may be held liable for failing to implement adequate security measures to protect patient information.

d. Due process

Due process ensures that individuals are treated fairly and justly in the use of information systems. It includes providing individuals with notice, consent, and the right to appeal decisions affecting them. In the context of employee performance evaluations, due process requires that employees receive notice of the evaluation process, the criteria used, and have the opportunity to provide their input or challenge negative assessments. This ensures a fair and transparent evaluation process.

e. Privacy

Privacy refers to an individual's right to control their personal information and to decide who has access to it. It involves safeguarding sensitive data from unauthorized access and ensuring that individuals' personal data is handled with care. An online retail company collects customer data, including names, addresses, and purchasing habits. It has an ethical obligation to protect this data from data breaches and to use it responsibly for legitimate purposes, such as order processing and personalized recommendations. Unauthorized sharing of this data without the customers' consent would be a privacy violation.

Laws and social practices in intellectual properties

a. Copyright

Intellectual property rights are statutory grants that prevent others from copying creators' work. Under the Copyright Act 1987, copyright owners, authors, and performers hold the right to control creative works created by them. Music compositions, maps, drawings, and artwork are all subject to copyright protection. By ensuring that creative people receive financial and other benefits from their work, copyright encourages creativity and authorship. It provides a protection for ideas that are expressed. Information systems are protected from copying or integrating software by Copyright laws. A patent can be obtained for software systems, methods, algorithms, and functions that the developer invented.

b. Patents

Patent law focuses on originality, novelty, and invention. Patents grant exclusive monopoly rights to invention ideas for 20 years. Inventions under U.S. patent law are meant to ensure that inventors receive full financial and other rewards for their work and that they can be widely used by providing detailed diagrams for those who would like to use them under license.

There is a significant advantage to patent protection in the sense that it grants a monopoly on the underlying concepts and ideas of software. This monopoly allows the owner of the patent to prevent competitors from developing, using, or selling the same software, allowing them to charge higher prices and dictate the terms of the market.

c. Trademarks

Generally, trademarks refer to the marks, symbols, or images used to distinguish one product from another within a market. The purpose of trademark laws is to protect consumers by ensuring that they receive what they paid for. As a result, trademark laws help to prevent fraud and promote fair competition in the marketplace. Moreover, these laws safeguard the investments that firms have made in order to bring products to market. An example of trademark infringement would occur if a firm copied the trademarked Google icon, colors, and images.

d. Trade secrets

Trade secrets are intellectual properties used for business purposes, such as formulas, devices, patterns, manufacturing processes, or data compilations, which are not derived from publicly available information. There may be a monopoly on a work product's ideas under a trade secret law, but this monopoly may not last long.

Malaysia's privacy and data protection law

In Malaysia, the Personal Data Protection Act 2010 (Act 709) is one of the most important pieces of cyber legislation. In accordance with the 10th policy goal, this act plays a pivotal role in ensuring information security and network reliability.

The Personal Data Protection Act 709 primarily governs the processing of personal data in commercial transactions, providing a protective net for a wide range of businesses, including banks, telecommunications companies, insurance companies, hospitals, and many more. In addition to safeguarding individuals' personal information, it also bolsters public confidence and trust through rigorous enforcement, thus adding prominence to its importance

IMPORTANCE OF THE ACT 709

- To enhance public confidence and trust with ongoing enforcement.
- To avoid and minimize the incidents of data breach.
- To increase the efficiency and g overnance of p ersonal data.
- To ensure prudence and integrity in personal data handling.

7 PRINCIPLES OF PDPA

1.General Principles

A data subject's consent is required for the processing of personal data.

2. Notice and choice principle

A data user is required to inform a data subject

- The user of data must inform the subject of their data
- The purpose for which personal data is processed, including the right of access, the disclosures of personal data to third parties, and the consequences of not providing such data.

3. Disclosure principle

Provides that personal data cannot be disclosed without the consent of the data subject

4. Security principle

During data processing, users must take steps to prevent loss, misuse, modification and destruction of personal data.

5. Retention principle

There must be reasonable measures taken to ensure that personal data is destroyed or permanently deleted if it is not required to keep it for the purpose it was processed.

6. Data Integrity Principle
An individual must ensure that their personal information is accurate, up-to-date, complete, and not misleading

7. Access Principle
Data subjects should have access to their own data and be allowed to correct inaccurate, incomplete, misleading and outdated information.

Terminology in PDPA related to DATA

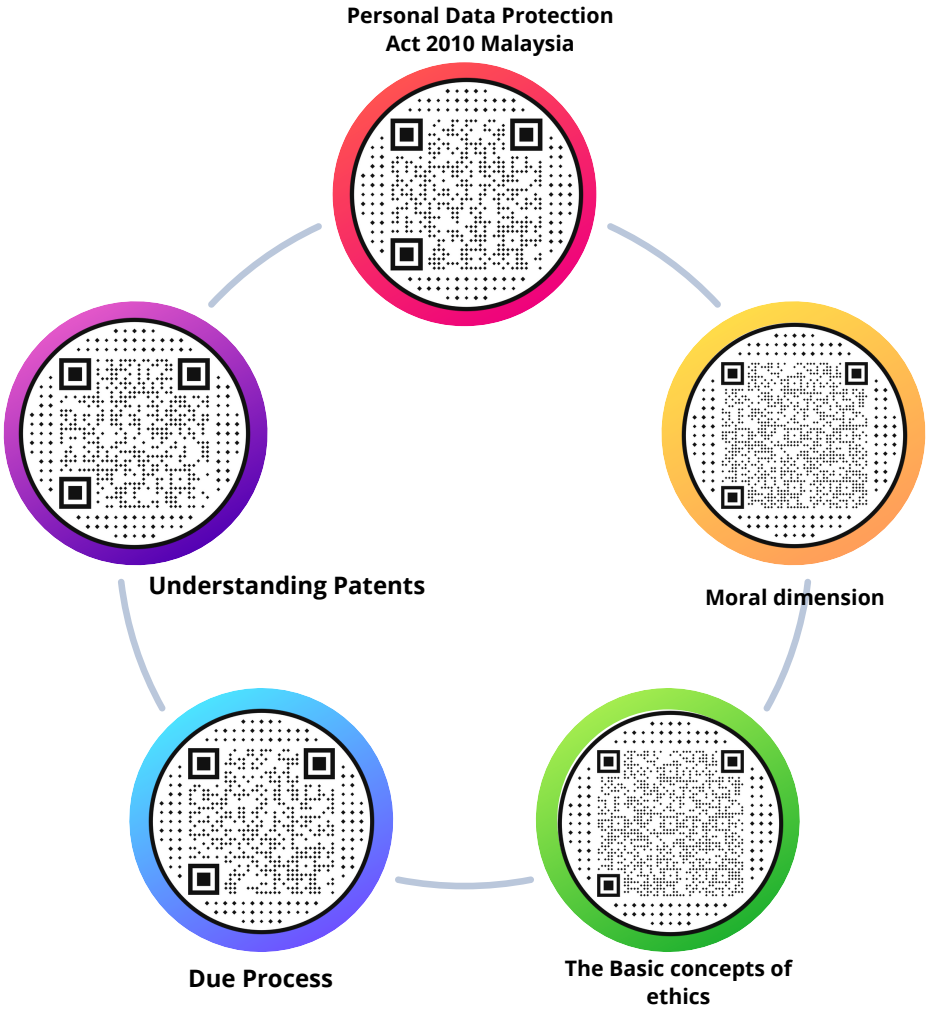
i. Data User
Anyone who processes personal data in relation to commercial transactions (whether an individual, a company, or an organization) or authorizes the processing

ii. Data Processor
Individuals who process personal data solely on behalf of the data user, other than employees of the data user

iii. Data Subject
A person whose personal data is being processed

Right of data Subjects

1. Right to block direct marketing processing
2. The right to prohibit processing that could harm or distress a person
3. The right to correct
4. The right to access
5. The right to revoke an agreement


Personal Data Protection Act 2010 Malaysia
Moral dimension
The Basic concepts of ethics
Due Process
Understanding Patents

QUIZ

PRACTICAL WORKSHEET 1

PRACTICAL WORKSHEET 2

PRACTICAL WORKSHEET 3

Bibliography

Kenneth C. Laudon & Jane P. Laudon (2021). Management Information Systems: Managing the Digital Firm. 17th Edition. Harlow, United Kingdom: Pearson Education Limited.

Kenneth C. Laudon & Jane P. Laudon (2021). Essentials of MIS. 14th Edition. Harlow, United Kingdom: Pearson Education Limited.

Jack A. Hyman (2022). Microsoft Power BI For Dummies. New Jersey, USA: John Wiley & Sons, Inc.

Lee Hurst (2020). Hands On With Google Data Studio. Indiana, USA: Wiley Publication.

Paige Baltzan & Amy Philips (2023). M: Information Systems. 7th Edition. United Kingdom: Mc Graw Hill.

Management Information System: Fundamentals

e ISBN 978-967-0032-91-7

UNIT PENERBITAN POLITEKNIK SULTAN SALAHUDDIN ABDUL AZIZ SHAH
(online)