NINJA NOTES

Information Systems & Control 2026

Introduction

Content Area Allocation

The following table summarizes the content areas and the allocation of content tested in the ISC section of the Exam:

Area I	Information Systems and Data Management	35% - 45%
Area II	Security, Confidentiality and Privacy	35% - 45%
Area III	Considerations for System and Organization Controls (SOC) Engagements	15% - 25%

Skill Allocation

Remembering and Understanding	55% - 65%
Application	20% - 30%
Analysis	10% - 20%
Evaluation	0% - 0%

Scoring Weight

The table below presents the scoring weight of MCQs and TBSs

	Multiple-Choice Questions (MCQs)	Tasked-Based Simulations (TBSs)
ISC - Discipline	60%	40%

Section Time and Question Type

The table below presents the design of the Exam by section time and question type.

	Section Time	Multiple-Choice Questions (MCQs)	Tasked-Based Simulations (TBSs)
ISC - Discipline	4 Hours	82	6

Content

NINJA NOTES

Information Systems & Control 2026

IT Infrastructure & Cloud Computing

Copyright & Disclaimer

This book is written to provide accurate and authoritative information concerning the covered topics for the Uniform CPA Examination and is to be used solely for studying for the Uniform CPA Examination and for no other purpose.

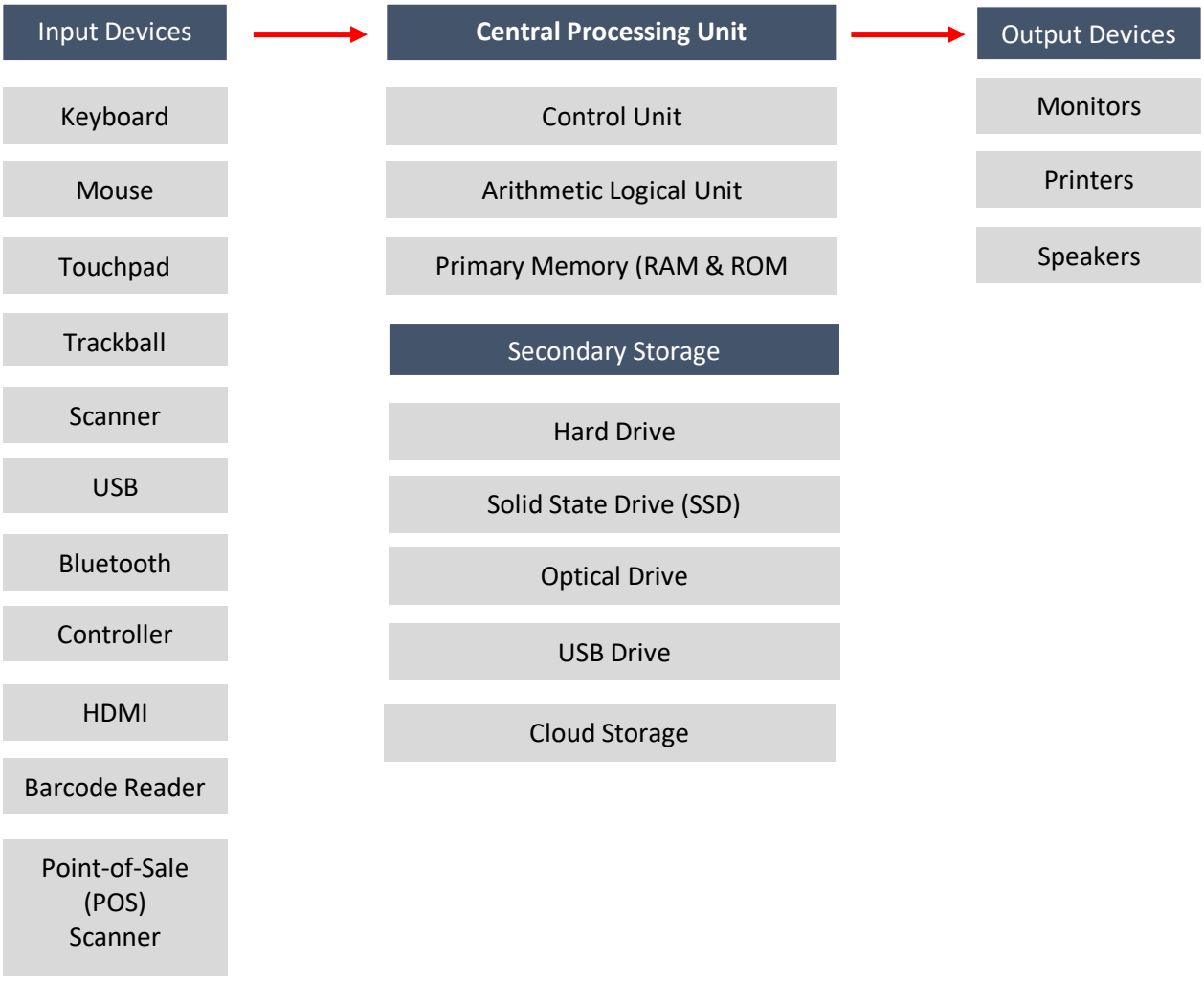
IT Infrastructure & Cloud Computing

IT Infrastructure

- Types of Computers
    - Supercomputers
        - Supercomputers are among the fastest computers currently available and are employed for specialized applications that require immense amounts of mathematical calculations
        - They are very expensive and are used for applications such as weather forecasting, scientific simulations, graphics, fluid dynamic calculations, nuclear energy research, electronic design, and analysis of geological data in petrochemical prospecting
    - Mainframe Computers
        - Mainframe Computers are very large and expensive computers capable of simultaneously supporting hundreds or even thousands of users
        - They were originally called mainframe computers because they contained the central processor unit in a large cabinet, but the term has come to encompass any large computer that is used for mainframe-type applications
    - Minicomputer
        - Minicomputers are larger and more powerful than a personal computer, but smaller and less powerful than a mainframe computer
        - These computers are typically used by small and medium-sized businesses and organizations for tasks such as file and print serving, database management, and application hosting
    - Microcomputers
        - Microcomputers, also known as Personal Computers (PCs), are small, relatively inexpensive computers that are designed for an individual user
        - They include desktops and laptops and are based on microprocessor technology, which enables manufacturers to put an entire CPU on one chip
    - Tablets
        - Tablets are portable computers that are small enough to be held in one's hand
        - They are convenient to carry and can be used instead of a laptop due to their processing power and on-screen keyboard

- Smartphones
  - Like a Tablet, but smaller
  - Advantages vs Tablet
    - Portability and Cell Service (many tablets are Wi-Fi only)
  - Disadvantages vs Tablet
    - Screen is too small for most business functions

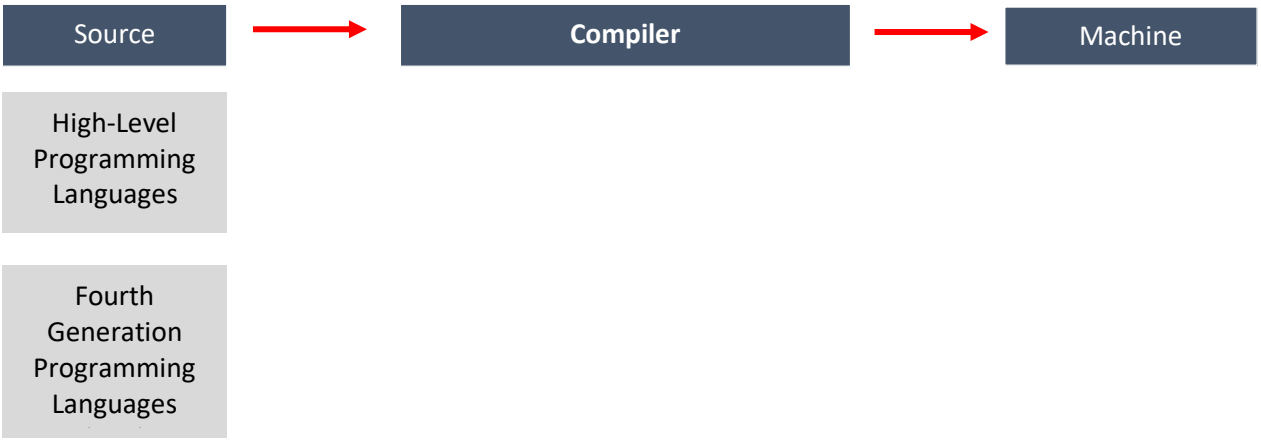
- Hardware



- Software
    - Software is a set of instructions that tells a computer what to do and how to do it. It is a collection of programs and data that enables a computer to perform specific tasks.
    - There are two main types of software: System Software and Application Software.
    - System Software
        - System Software is software that manages and controls the hardware and other system resources of a computer.
        - Operating System
            - Operating System is the most important type of system software.
            - The Operating System manages the Hardware and Software resources of a computer and provides a platform for running application software.
        - Utility Programs
            - Utility Programs are a type of system software that are designed to perform specific tasks, such as virus scanning, disk defragmentation, and data backup.
                - ⇒ Antivirus Software
                - ⇒ Disk Defragmenter
                - ⇒ Backup Software
                - ⇒ System Monitoring Software
                - ⇒ Disk Cleanup Utility
    - Application Software
        - Application Software is software that is designed to perform specific tasks, such as word processing, spreadsheet management, and photo editing.
        - Productivity Software
            - Examples include word processors, spreadsheet programs, and presentation software.
        - Graphics Software
            - Examples include photo editing software, illustration software, and 3D modeling software.

- Multimedia Software
  - Examples include audio editors, video editors, and music production software.
- Communication Software
  - Examples include email clients, chat programs, and video conferencing software.
- Games
- Heuristic Software
  - Heuristic Software is software that uses heuristic algorithms or methods to solve problems or make decisions.

- Programming Language
  - A Programming Language is a set of instructions, rules, and conventions that are used to create and execute Software Programs.
  - It is a way of communicating with a computer and giving it specific instructions to perform a task.



  - Machine Language
    - Machine language, also known as machine code or assembly language, is a set of instructions that are written in a form that can be directly executed by a computer's Central Processing Unit (CPU).
    - Machine language consists of a series of binary digits (ones and zeros) that represent the instructions and data that the computer is to process.

- Source Program

  - A Source Program is a set of instructions written in a programming language that is intended to be compiled or interpreted by a computer.

  - The Source Program is written in High-Level Programming Languages or Fourth Generation Programming Languages (4GL).

  - High-Level Programming Languages

    - High-level Programming Languages are programming languages that are designed to be more human-readable and easier to use than machine language.

    - They are closer to natural human language and are less detailed and more abstract than Machine Language.

      ⇒ C

      ⇒ C++

      ⇒ Java

      ⇒ Python

      ⇒ JavaScript

  - Fourth Generation Programming Languages (4GL)

    - Fourth-Generation Programming Languages (4GLs) are a type of High-Level Programming Language that is designed to be more user-friendly and easier to use than Traditional Programming Languages.

    - 4GLs are characterized by their use of English-like statements and commands, which make them easier to read and understand than traditional programming languages.

- Compiler

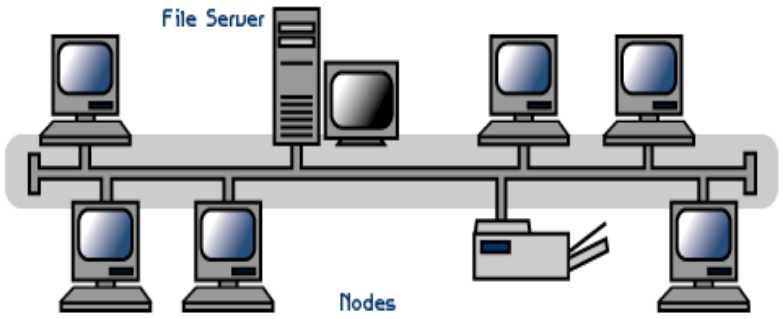
  - A Compiler is a type of software that converts source code written in a programming language into machine code that can be executed by a computer.

- Network
    - A Network allows devices to connect and communicate with each other, enabling the exchange of data and information.
    - Types of Networks – Based on Geographical Coverage
        - Personal Area Network (PAN)
            - A Personal Area Network (PAN) is a type of network that connects devices and other personal computing devices that are close to a person, typically within a range of a few meters.
        - Local Area Network (LAN)
            - A Local Area Network (LAN) is a network that connects devices within a limited geographic area, such as a home, office, or school.
        - Wireless Local Area Network (WLAN)
            - A Wireless Local Area Network (WLAN) is a type of LAN that uses wireless technology, such as Wi-Fi, to connect devices.
        - Value-Added Network (VAN)
            - A Value-Added Network (VAN) is a type of network that provides value-added services, such as data storage and secure transmission, to businesses and organizations.
        - Wide Area Network (WAN)
            - A Wide Area Network (WAN) is a network that connects devices over a large geographic area, such as a city, country, or the entire world.
            - The Internet is the largest WAN, connecting millions of devices worldwide.
    - Types of Networks – Based on Ownership
        - Private Networks
            - Private Networks are networks that are owned and operated by a single organization or entity and are typically used to connect devices within that organization.
            - Advantages
                - ⇒ Increased Security
                - ⇒ Flexibility
                - ⇒ Better Performance

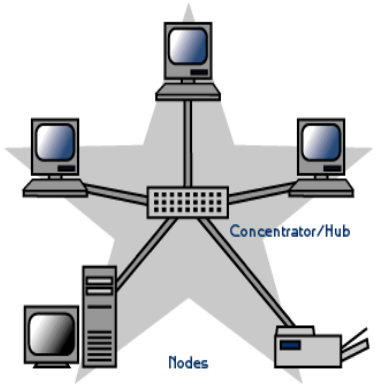
- Disadvantages
  - ⇒ Higher Cost
  - ⇒ Limited Access
  - ⇒ Limited Scalability

- Public Networks
  - Public Networks, on the other hand, are networks that are owned and operated by third-party companies and leased to users on a usage basis.
  - Advantages
    - ⇒ Lower Cost
    - ⇒ Wider Availability
    - ⇒ Scalability
  - Disadvantages
    - ⇒ Lower Security
    - ⇒ Lower Performance
    - ⇒ Limited Control

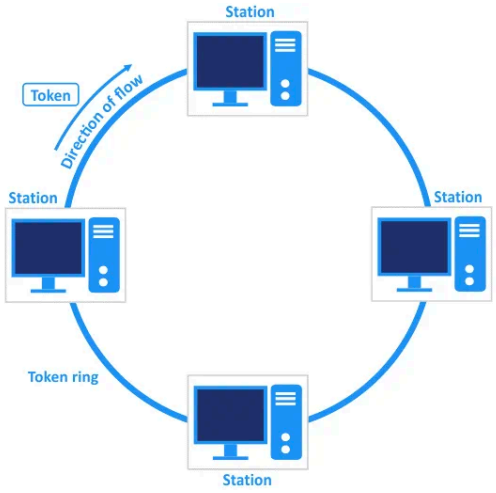
- Network Topology
  - Network Topology refers to the shape or layout of a network and determines how devices on the network are connected to each other and how they communicate.
  - Bus Topology



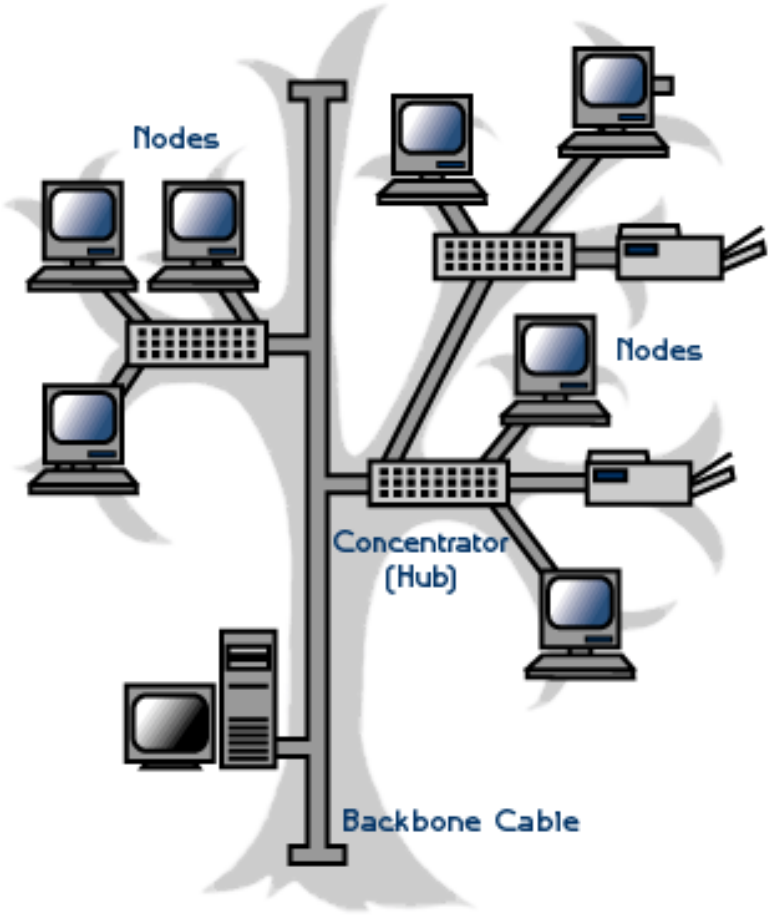
- Star Topology



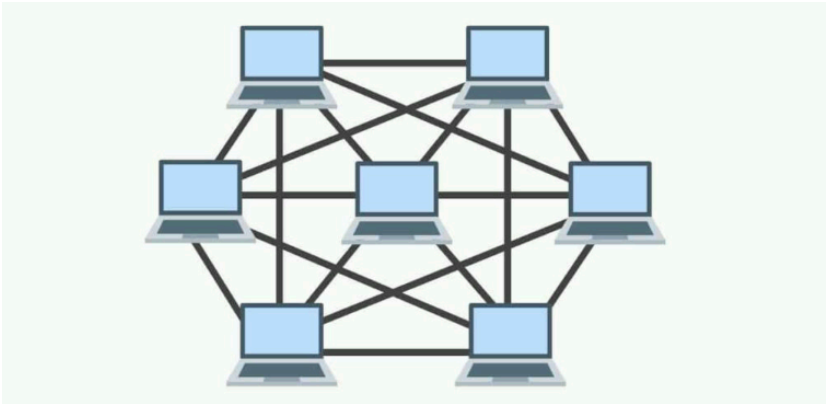
- Ring Topology



- Tree Topology



- Mesh Topology



- Client-Server Architecture

  - In Computer Networking, the Client-Server Architecture is a standard model of communication where one device (The Server) is responsible for providing a specific service to other devices (The Clients).

  - The client sends a request to the server, which then performs a specific task and sends a response back to the client. This model is commonly used for applications such as email, file sharing, and web services. The client-server architecture can be implemented on a local area network (LAN) or over the Internet.

  - Client

    - In a Client-Server Architecture, clients are typically individual computers or workstations that are used by users to access the resources provided by the server.

  - Server

    - The Server is a high-capacity computer that contains the necessary software and hardware to provide a variety of services to the clients.

- Internet

  - The Internet is a global network of interconnected computers and servers that communicate with each other.

  - Internet Related Terminologies

    - Intranet

      - An Intranet is a private network that is used by an organization to share information and resources among its employees, members, or departments.

    - Extranet

      - An Extranet is a private network that shares part of an organization's information or operations with suppliers, vendors, partners, customers, or other businesses.

    - World Wide Web

      - The World Wide Web (WWW or Web) is a vast network of interconnected documents and other resources, linked by hyperlinks and URLs.

      - It is the primary platform for information-sharing on the Internet and is used by billions of people every day to access information, communicate, and conduct business.

- Hyper-Text Transfer Protocol (HTTP)
  - HTTP is a protocol used for transferring data over the Internet.
- Transmission Control Protocol/Internet Protocol
  - TCP/IP stands for Transmission Control Protocol/Internet Protocol, and it is the basic communication protocol of the Internet.
  - TCP is responsible for ensuring that data is transmitted reliably and in the correct order, while IP is responsible for routing data packets to their destination.
- Internet Service Provider (ISP)
  - An Internet Service Provider (ISP) is a company that provides customers with access to the Internet.
- Uniform Resource Locator (URL)
  - A Uniform Resource Locator (URL) is a unique string of characters that identifies a specific webpage or resource on the Internet.
  - A URL is often called a web address, and it is used to locate and retrieve a specific resource, such as a webpage, image, or video.
- Web Servers
  - Web Servers are specialized computers that store and manage webpages, images, videos, and other types of data on the Internet.
- Web Browser
  - A Web Browser is a software application that allows users to access and navigate the World Wide Web.
- Router
  - A Router is a connection point between a home or office network and the Internet.
- Gateway
  - A Gateway is a networking device that connects two different networks together, allowing them to communicate with each other.
- Bridge
  - A Bridge is a networking device that connects two separate LANs (Local Area Networks) together, allowing them to communicate with each other as if they were a single network.

- Switch
  - A Switch is a networking device that connects multiple devices together on a computer network and forwards data packets between them.
- Proxy Server
  - A Proxy Server is a server that acts as an intermediary between a client and a server in a network.
  - It forwards requests from clients to servers and returns the responses back to the clients.
- Killer Application
  - A Killer Application, also known as a "killer app", is a software program that is so useful and in demand that it drives the sales of a particular hardware platform or operating system
  - For example, a spreadsheet program like Microsoft Excel or Google Sheets can be considered as a Killer application for personal computers, as it is so widely used and necessary for many businesses and individuals.
- HTML (Hypertext Markup Language)
  - HTML (Hypertext Markup Language) is a markup language used to create the structure and layout of a webpage.
- XML (eXtensible Markup Language)
  - XML (eXtensible Markup Language) is a markup language used to store and transport data.
  - XML (eXtensible Markup Language) is similar to HTML in that it is a markup language used to structure and organize data.
- XBRL (eXtensible Business Reporting Language)
  - XBRL (eXtensible Business Reporting Language) is a standard for electronic communication of business and financial data.
  - XBRL allows companies to tag financial data in their reports using a standardized set of tags, called taxonomies, which define the meaning of the data.
  - This makes it possible for financial software and other applications to automatically extract and analyze the data, reducing the need for manual data entry and increasing the accuracy of the analysis.

- Security Threats on Internet
  - Virus
    - A Virus is a type of malware (malicious software) that attaches itself to a legitimate program or file and is designed to replicate and spread itself to other computers.
  - Trojan Horse
    - A Trojan horse is a type of malware that disguises itself as a legitimate program or file, but once executed, it can cause damage or steal information from the infected computer.
  - Worm
    - A Worm is a type of malware that is similar to a virus in that it replicates itself and can spread to other computers, but it does not need to attach itself to a legitimate program or file to do so.
  - Hoax Virus
    - A Hoax Virus is a message that is circulated through email or social media warning users of a virus that does not actually exist.
  - Phishing
    - Phishing is a type of social engineering attack that is used to trick users into providing sensitive information, such as passwords, credit card numbers, or personal details.
- Protection against Security Threats on Internet
  - Firewall
    - A Firewall is a security system that is used to control incoming and outgoing network traffic by analyzing data packets and determining whether they should be allowed through or not.
    - Firewalls can be Network Firewall and Application Firewall:
    - Network Firewall
      - ⇒ A Network Firewall is implemented at the network level, which means it controls all the traffic that flows in and out of the network.
      - ⇒ It uses security algorithms and router communications protocols to prevent outsiders from accessing the corporate database and e-mail systems.
    - Application Firewall
      - ⇒ An Application Firewall, on the other hand, is implemented at the application level.

⇒ It controls the traffic that flows in and out of specific programs or applications.

- Antivirus Software
  - Antivirus Software is a program or set of programs that are designed to prevent, detect, and remove malware from a computer or mobile device.
- Virtual Private Network (VPN)
  - A Virtual Private Network (VPN) is a technology that allows users to securely connect to a private network over the Internet.

Cloud Computing

- Cloud Computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("The Cloud") to offer faster innovation, flexible resources, and economies of scale.
- Examples of Cloud Computing providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- Types of Cloud
  - Private Cloud
    - A Private Cloud is a cloud computing environment that is dedicated to a single organization.
  - Community Cloud
    - A Community Cloud is a type of cloud computing environment that is shared by a specific group of organizations with similar requirements and concerns.
  - Public Cloud
    - A Public Cloud is a type of cloud computing environment where resources, such as servers, storage, and applications, are made available to the general public over the Internet.
    - Public Clouds are owned and operated by third-party companies, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
  - Hybrid Cloud
    - A Hybrid Cloud is a type of cloud computing environment that combines the benefits of both public and private clouds.

- Cloud Computing Service Models
    - Cloud Computing Service Models are categorized based on the type of access and ownership of the underlying infrastructure
    - Infrastructure as a Service (IaaS)
        - Infrastructure as a Service (IaaS) is a type of cloud computing service model that provides virtualized computing resources, such as servers, storage, and networking, over the Internet.
        - Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
    - Software as a Service (SaaS)
        - Software as a Service (SaaS) is a type of cloud computing service model that provides software applications over the Internet, which can be accessed on demand.
        - SaaS is a delivery model where software vendors host and maintain their software applications and make them available to customers over the Internet.
        - Examples of SaaS providers include Office 365, Salesforce, Zoom, G-Suite, Adobe Creative Cloud, Slack, and many more.
    - Platform as a Service (PaaS)
        - Platform as a Service (PaaS) is a type of cloud computing service model that provides a platform for developing, running, and managing applications without the need for users to worry about the underlying infrastructure.
        - Examples of PaaS providers include Heroku, Salesforce App Cloud, Google App Engine, AWS Elastic Beanstalk, and Azure App Service.
- Roles and Responsibilities of Cloud Service Providers
    - Infrastructure Management
        - Cloud Service Providers are responsible for setting up, maintaining, and managing the physical infrastructure required to deliver cloud services.
    - Resource Provisioning
        - One of the primary responsibilities of a Cloud Service Provider is to provide on-demand computing resources, such as processing power, memory, storage, and networking.
    - Service Reliability and Availability
        - Cloud Service Providers must ensure that their services are reliable and available to their customers.

- Security and Compliance
    - Cloud Service Providers are responsible for implementing robust security measures to protect their customers' data and applications.
- Platform and Software Management
    - In the case of PaaS and SaaS offerings, cloud Service Providers are responsible for managing the underlying platforms and software applications, respectively.
- Customer Support and Service
    - Cloud Service Providers are responsible for providing customer support and assistance, which may include technical support, documentation, training, and consulting services.
- Billing and Cost Management
    - Cloud Service Providers offer flexible, pay-as-you-go pricing models, which require them to monitor and track customers' resource usage accurately.
- Service-Level Agreements (SLAs)
    - Cloud Service Providers establish Service-Level Agreements (SLAs) with their customers, outlining the performance, availability, and support standards they commit to.
- Innovation and Scalability
    - Cloud Service Providers must continuously innovate and improve their services to stay competitive in the rapidly evolving cloud computing landscape.

- Cloud Computing Governance
    - Cloud Computing Governance refers to the process of establishing and implementing a set of policies, procedures, and guidelines to ensure that an organization's cloud computing resources are effectively managed, secure, compliant, and aligned with its overall business objectives.
    - Cloud Computing Governance encompasses several key elements, including:
        - Strategy and Goals
            - Defining the organization's cloud computing strategy, aligning it with business objectives, and setting clear goals for cloud adoption, migration, and management
        - Risk Management
        - Policies and Procedures

        - Establishing and documenting cloud-specific policies, procedures, and guidelines that cover areas like data management, security, privacy, and vendor management

    - Roles and Responsibilities
        - Defining and assigning roles and responsibilities for cloud governance within the organization.
    - Compliance and Legal Requirements
        - Ensuring that the organization's cloud computing activities comply with relevant laws, regulations, and industry standards, such as GDPR, HIPAA, and SOC 2.
    - Vendor Management
    - Performance Measurement and Monitoring
    - Training and Awareness
    - Incident Management and Response

- Role of COSO Frameworks in Cloud Computing Governance
    - Role of COSO Internal Control Framework in Cloud Computing Governance
        - Control Environment
            - Establish a strong Control Environment for cloud computing by setting a tone at the top that emphasizes the importance of cloud security, compliance, and risk management.
        - Risk Assessment
            - Conduct a comprehensive Risk Assessment to identify and prioritize cloud-related risks, such as data security, privacy, vendor management, regulatory compliance, and operational risks.
        - Control Activities
            - Implement cloud-specific control activities to mitigate identified risks, such as access controls, data classification, encryption, intrusion detection and prevention systems, and incident response plans.
        - Information and Communication
            - Develop effective communication channels to share relevant information about cloud governance, such as policies, procedures, and risk assessments, both within the organization and with external stakeholders.

- Monitoring Activities
    - Establish a Monitoring program to evaluate the effectiveness of cloud governance efforts, including the performance of control activities and the organization's adherence to cloud-related policies and procedures.

- Role of COSO Enterprise Risk Management Framework in Cloud Computing Governance
    - Governance and Culture
        - Establish a strong risk culture for cloud computing by setting a tone at the top that emphasizes the importance of cloud security, compliance, and risk management.
        - Define clear roles and responsibilities for managing cloud resources and embed risk awareness throughout the organization.
        - Develop risk appetite and tolerance statements specific to cloud computing and ensure they are aligned with the organization's overall risk appetite and strategic objectives.
    - Strategy and Objective Setting
        - Integrate cloud computing risks and opportunities into the organization's strategy-setting process.
    - Performance
        - Identify, assess, and prioritize cloud-related risks and opportunities, such as data security, privacy, vendor management, regulatory compliance, and operational risks.
        - Establish risk tolerances, risk response strategies, and performance metrics to monitor risk management effectiveness for cloud computing.
    - Review and Revision
        - Continuously evaluate and improve the organization's cloud computing governance and risk management practices, identifying and addressing deficiencies and gaps, learning from past events, and enhancing risk management capabilities.
    - Information, Communication, and Reporting
        - Ensure that relevant and timely risk-related information for cloud computing is identified, captured, and communicated within the organization and to external parties.
        - Enable all personnel to understand their risk management responsibilities, adhere to cloud governance requirements, and make informed decisions.
        - Develop information systems and communication channels that support the flow of information, both vertically and horizontally, across the organization.