**Assignment #1 – Cloud Computing Fundamentals**

**Tasks:**

* What is cloud computing, and how does it differ from traditional IT infrastructure?

**Purpose:**

* Define: Understand the core concepts of cloud computing and traditional IT infrastructure.
* Compare: Identify the key differences between cloud computing and traditional IT infrastructure models.

Cloud computing is a technology that enables users to access computing resources (such as servers, storage, databases, networking, software, and analytics) over the Internet on a pay-as-you-go basis. In contrast, traditional IT infrastructure typically involves procuring and maintaining physical hardware and software within an organization's data centers or on-premises locations. Cloud computing offers scalability, flexibility, and cost-effectiveness compared to traditional IT setups' capital-intensive and less agile nature.

**Assignment #2 – Cloud Computing Fundamentals**

**Tasks:**

* Explain the concept of the shared responsibility model in cloud computing security.

**Purpose:**

* Define: Understand the core concept of the shared responsibility model in cloud computing.
* Analyze: Evaluate the distribution of responsibilities between cloud service providers and customers in ensuring security.

The shared responsibility model in cloud computing outlines the division of security responsibilities between the cloud service provider and the customer. The provider is responsible for securing the underlying cloud infrastructure, while the customer is responsible for ensuring their data, applications, and configurations within the cloud environment. Understanding these shared responsibilities is crucial for maintaining a secure cloud environment.

**Assignment #3 – Cloud Computing Fundamentals**

**Tasks:**

* What are the three main service models in cloud computing, and how do they differ from each other?

**Purpose:**

* Identify: Recognize the primary service models in cloud computing.
* Differentiate: Understand the distinctions between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The three main service models in cloud computing are:

* **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet.
* **Platform as a Service (PaaS):** Offers hardware and software tools over the internet, primarily for application development.
* **Software as a Service (SaaS):** Delivers software applications over the internet on a subscription basis.

Each model differs in terms of the level of abstraction and management provided by the cloud provider, the scope of responsibility for the customer, and the flexibility and scalability of the services offered.

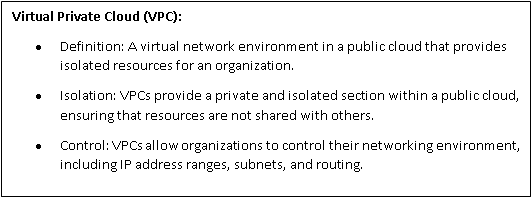
**Assignment #4 – Cloud Computing Fundamentals**

**Tasks:**

* Define Virtual Private Cloud (VPC) in cloud computing.
* Explain how VPCs provide isolation and control in the cloud.

**Purpose:**

* Define: Understand the concept of Virtual Private Cloud (VPC).
* Explain: Describe the mechanisms by which VPCs ensure isolation and control in cloud environments.



**Assignment #5 – Cloud Computing Fundamentals**

**Tasks:**

* Describe the purpose and functionality of security groups in cloud computing environments.

**Purpose:**

* Define: Understand the role of security groups in cloud environments.
* Explain: Describe how security groups control network traffic in cloud deployments.

**Purpose and Functionality of Security Groups:**

* Definition: Security groups act as virtual firewalls that control inbound and outbound traffic for instances within a cloud environment.
* Access Control: Security groups allow users to define rules that permit or deny specific types of traffic based on source IP addresses, destination ports, and protocols.
* Instance-Level Protection: Each instance in a cloud deployment can be associated with one or more security groups, enabling fine-grained control over network access.
* Dynamic Updates: Changes to security group rules take effect immediately, allowing for dynamic adjustment of security policies in response to evolving threats or operational requirements.