1.) Explain the importance of implementing secure identity and access management (IAM) in a cloud environment. How does IAM help organizations control user access and permissions within cloud services, and what security risks can it mitigate?

Answer: Cloud based IAM enables the creation of user and user security groups, plus role-based management privileges, so that's what the IAM is important to management in the cloud environment. You are literally giving someone authority to login and have permissions. The IAM helps organizations to group permissions for their users so that they are not subject to privilege escalation attacks.

2) Discuss the concept of encryption in cloud security. How does encryption help protect data in transit and at rest within cloud services? Explain the difference between client-side and server-side encryption in a cloud context and provide an example of when each might be used.

Answers: Cloud storage utilizes the on-premises concept of Full Disk Encryption. Each storage unit is encrypted using an AES key. If an attacker were to physically access a data center and copy or remove a disk, that's a form of data at rest, they would not be able to read the data. Client-side encryption is when the host is encrypting data such as full disk encryption. Server-side encryption is when the server is encrypting data using technologies such as AES.