AWS Shared Responsibility Model

- Security and Compliance is a shared responsibility **between AWS and the customer.**

- This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

- The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

- Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

- The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment.

- As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.

CUSTOMER	CUSTOMER DATA			
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD	PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT			
	OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION			
	CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)		NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS	SOFTWARE			
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD	COMPUTE	STORAGE	DATABASE	NETWORKING
	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	REGIONS	AVAILABILITY ZONES		EDGE LOCATIONS