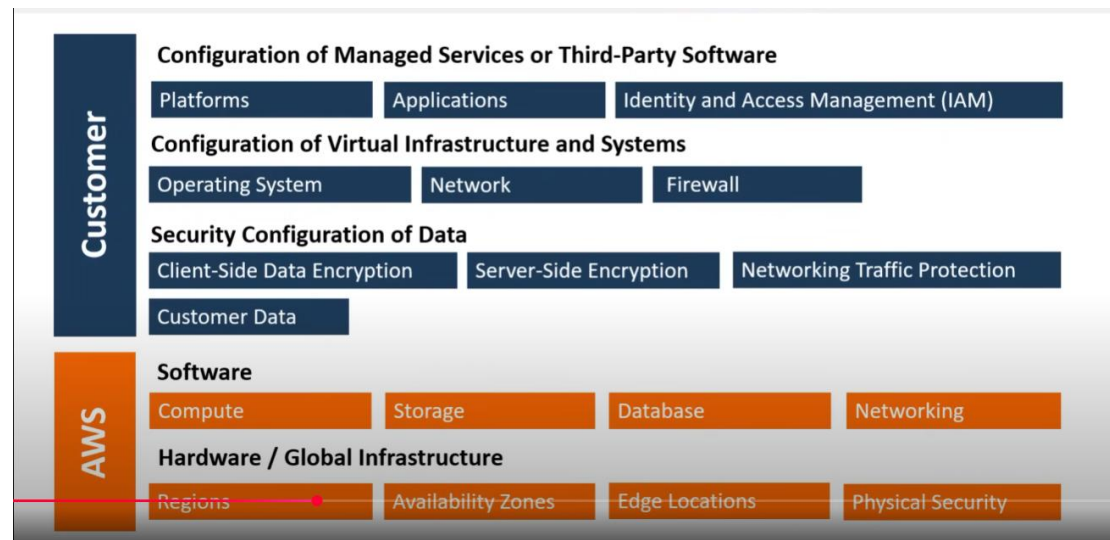
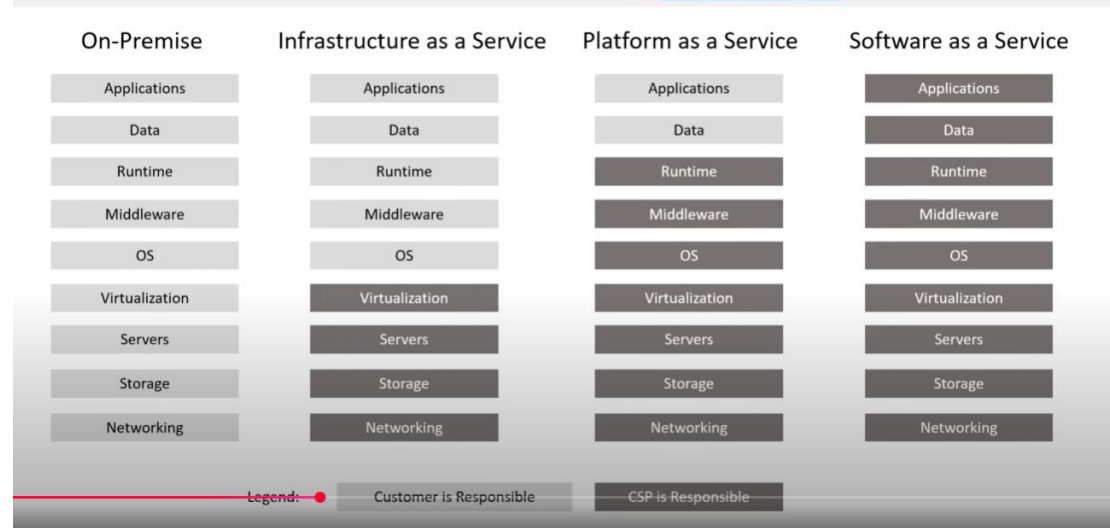


The Shared responsibility is a cloud security framework that defines the security obligations of the customer versus the CSP



In simple terms the customer bears the responsibility for what goes in the cloud and CSP bears the responsibility of the cloud

Eg for Computing



Let us take a look at **compute** as a comparison example of the Shared Responsibility Model

#### Infrastructure as a Service (IaaS)



**Bare Metal**  
EC2 Bare Metal Instance

Customer:

- The Host OS Configuration
- Hypervisor

AWS

- Physical machine



**Virtual Machine**  
Elastic Cloud Compute (EC2)

Customer:

- The Guest OS Configuration
- Container Runtime

AWS

- Hypervisor, Physical machine



**Containers**  
AWS Elastic Container Service(ECS)

Customer:

- Configuration of containers
- Deployment of Containers
- Storage of containers

AWS

- The OS, The Hypervisor, Container Runtime

#### Platform as a Service (PaaS)



**Managed Platform**  
AWS Elastic Beanstalk

Customer:

- Uploading your code
- Some configuration of environment
- Deployment strategies
- Configuration of associated services

AWS

- Servers, OS, Networking, Storage, Security

#### Software as a Service (SaaS)



**Content Collaboration**  
Amazon WorkDocs

Customer:

- Contents of documents
- Management of files
- Configuration of sharing access controls

AWS

- Servers, OS, Networking, Storage, Security

#### Function as a Service (FaaS)



**Functions**  
AWS Lambda

Customer:

- Upload your code

AWS

- Deployment, Container Runtime, Networking, Storage, Security, Physical Machine, (basically everything)