AWS Shared Responsibility Model

What is the AWS Shared Responsibility Model?

The shared responsibility between AWS and the customer is “security and compliance.” The AWS shared responsibility model is a concept that divides responsibilities between AWS and the customer. From the host operating system and virtualization layer to the physical security of the buildings where the service is hosted, AWS runs, oversees, and regulates every component. The guest operating system (including updates and security patches), other related application software, and the setup of the security group firewall offered by AWS are all under the customer's control and responsibility. In addition, customers must abide by the laws and regulations while considering the services and the duties.

To simplify, AWS's responsibilities are the security of the cloud, and customers' responsibilities are security in the cloud.

The following diagram differentiates the role of AWS and Customer as Security “of” the Cloud versus Security “in” the Cloud respectively.

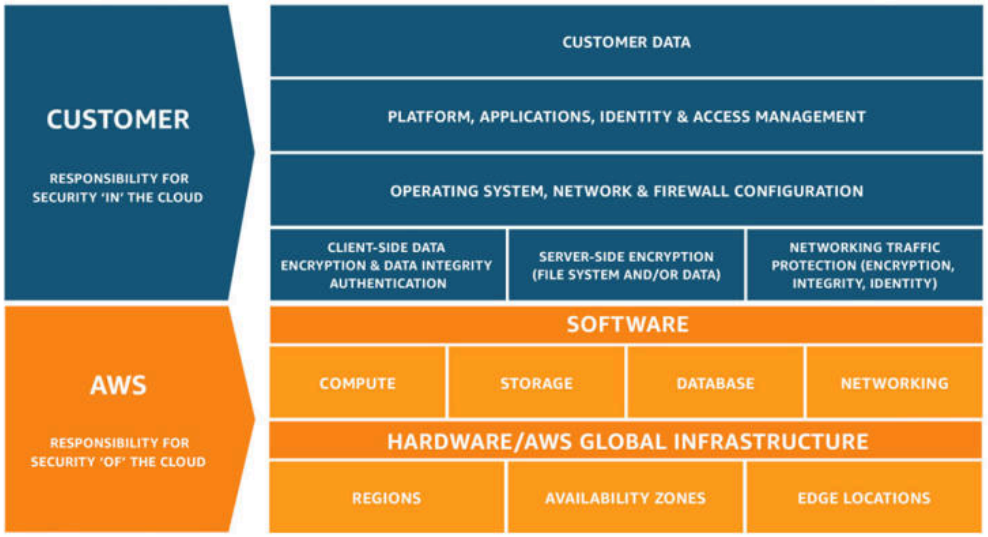

Figure 1.1 General AWS Shared Responsibility Model

1. **AWS responsibility "Security of the Cloud":**

- AWS's responsibility is the security of the cloud.
- AWS manages all infrastructure layers.
- Some of the infrastructure layers are:
- Data centers
- Hardware and software
- Virtualization
- Networking

2. **Responsibility of a Customer "Security in the Cloud":**

- Customers' responsibility is the security of everything they create in the AWS Cloud.
- Customers have complete control over your content.
- Customer manages AWS services, software, and access to the data.

Some key responsibilities of both parties:

For a clearer understanding, let us look at the following diagram and distinguish each's responsibility:

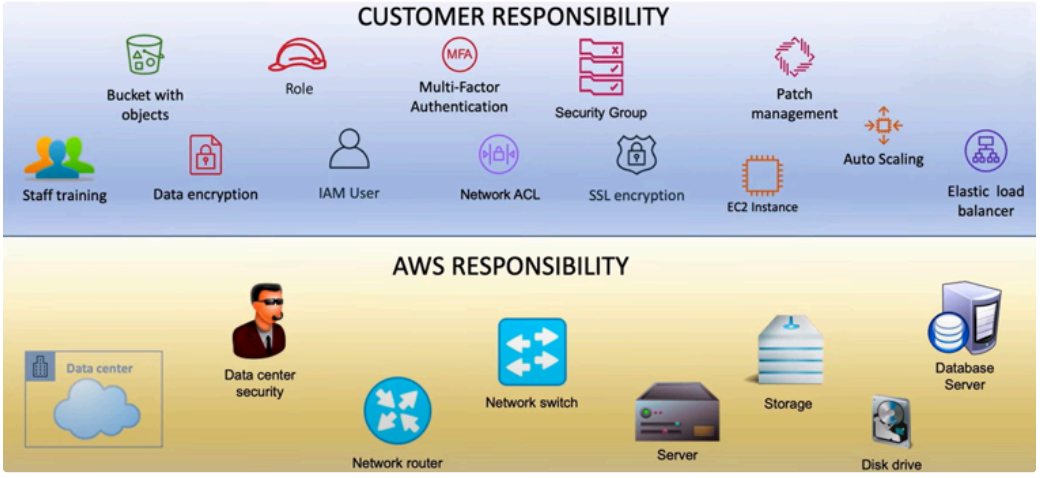

Figure 1.2 Services to be handled by both parties

The key responsibilities of AWS and the customer are shown in the table below:

AWS	Customer
Edge locations	Networking traffic protection
Availability zones	Server-side encryption

Regions	Client-side data encryption
AWS global infrastructure	Operating systems configuration
Hardware	Network configuration
Networking	Firewall configuration
Database	Platform management
Storage	Applications management
Compute	Identity management
Software	Access management
	Customer data

Shared Responsibility Model as an IT Control:

This customer/AWS shared responsibility model also extends to IT controls. IT controls are managed, run, and verified collaboratively. Customers can benefit from moving management of certain IT controls to AWS, which creates a (new) distributed control environment. Customers can then complete their control evaluation and verification processes as needed by using the AWS control and compliance documentation that is at their disposal. Some of the controls are explained below:

1. **Inherited Controls** – Controls that a customer fully inherits from AWS.

- Physical and Environmental Controls

2. **Shared Controls** – Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure, and the customer must provide their control implementation within their use of AWS services.
   Examples include:

   Patch Management:

- AWS - patching and fixing flaws within the infrastructure
- customers - patching their guest OS and applications.

Configuration Management:

AWS - configuration of its infrastructure devices

customers - configuring their own guest operating systems, databases, and applications.

Awareness & Training;

- AWS trains AWS employees, but,
- The customer must train their employees.

Customer Specific – Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security, which may require a customer to route or zone data within specific security environments.

Shared Responsibility Model and Service Categories

AWS provides various services that cause the line between security *"of"* and *"in"* the Cloud to shift relative to responsibility.

To understand it, let us look at the following diagram:

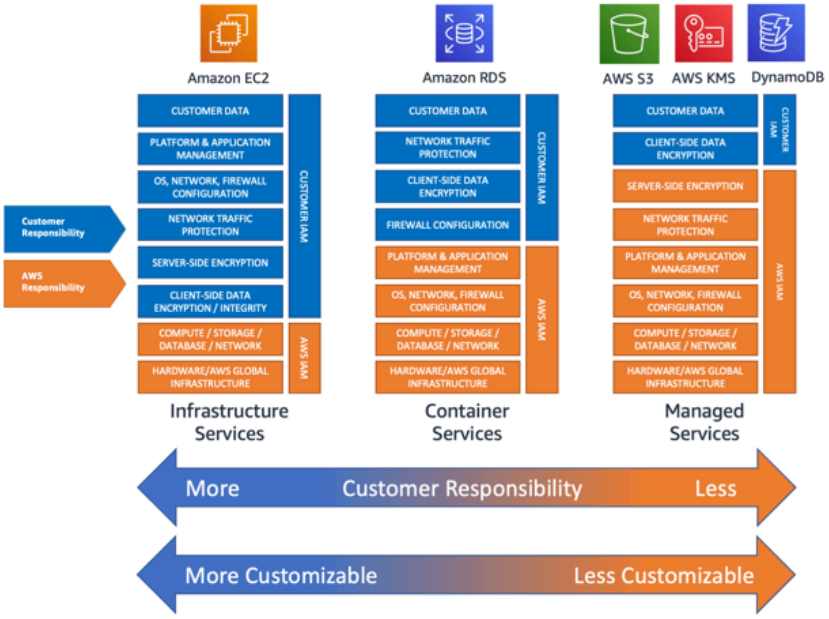

Figure 1.3 Shared Responsibility by Service Type

For different services provided by AWS, the range of shared responsibility varies from low to high. As shown in the diagram above, we can see that for AWS services like EC2 and RDS, there is high customer responsibility, while moving towards managed services like Amazon S3, DynamoDB, AWS KMS etc, the customer responsibility becomes less, and as a result, the customers will have lower degree of customization.

References:

Shared Responsibility Model - Amazon Web Services (AWS)

Applying the AWS Shared Responsibility Model to your GxP Solution | Amazon Web Services

Simplify the AWS Shared Responsibility Model

What is the AWS Shared Responsibility Model?