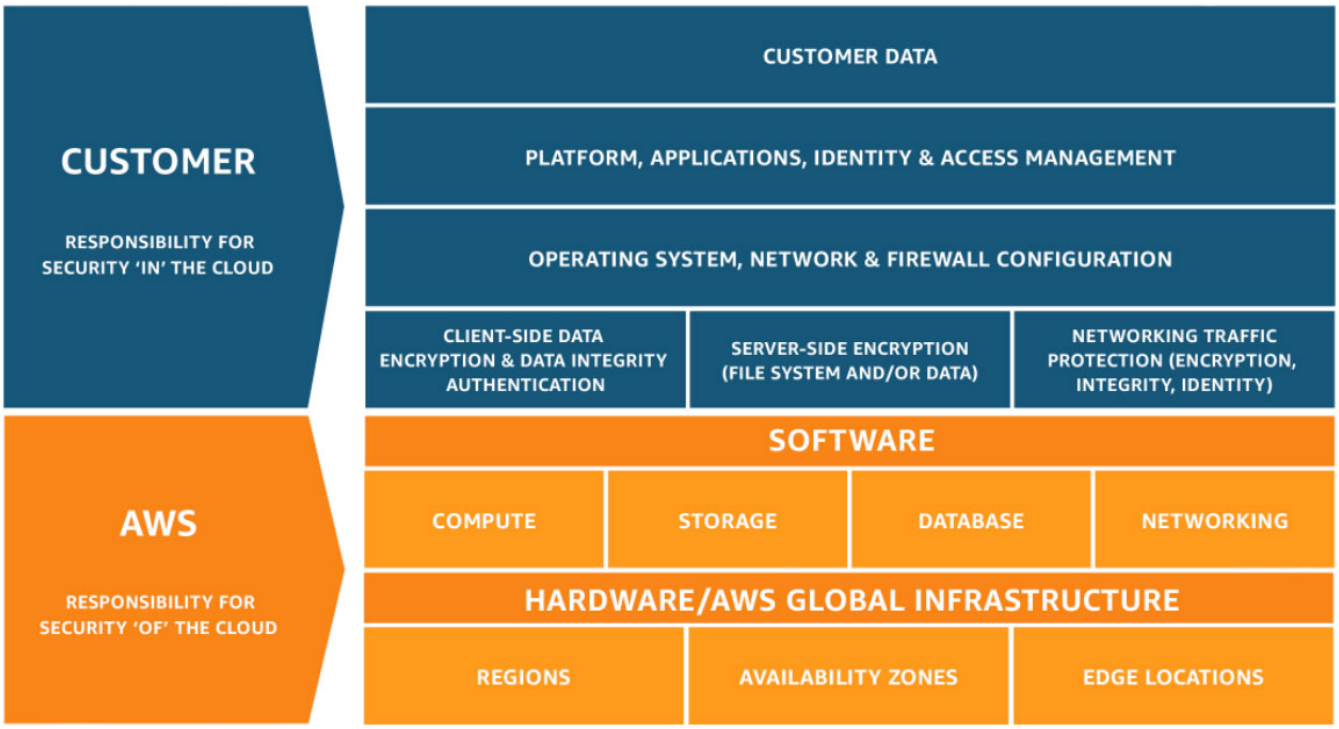
Reading 1.5: Security and the AWS Shared Responsibility Model

When you begin working with the AWS Cloud, managing security and compliance is a shared responsibility between AWS and you. To depict this shared responsibility, AWS created the shared responsibility model. This distinction of responsibility is commonly referred to as security of the cloud, versus security in the cloud.



What Is AWS Responsible For?

AWS is responsible for security of the cloud. This means AWS is required to protect and secure the infrastructure that runs all the services offered in the AWS Cloud. AWS is responsible for:

- Protecting and securing AWS Regions, Availability Zones, and data centers, down to the physical security of the buildings
- Managing the hardware, software, and networking components that run AWS services, such as the physical server, host operating systems, virtualization layers, and AWS networking components

The level of responsibility AWS has depends on the service. AWS classifies services into three different categories. The following table provides information about each, as well as the AWS responsibility.

Category	Examples of AWS Services in the Category	AWS Responsibility

Category	Examples of AWS Services in the Category	AWS Responsibility
Infrastructure services	Compute services, such as Amazon Elastic Compute Cloud (Amazon EC2)	AWS manages the underlying infrastructure and foundation services.
Container services	Services that require less management from the customer, such as Amazon Relational Database Service (Amazon RDS)	AWS manages the underlying infrastructure and foundation services, operating system, and application platform.
Abstracted services	Services that require very little management from the customer, such as Amazon Simple Storage Service (Amazon S3)	AWS operates the infrastructure layer, operating system, and platforms, as well as server-side encryption and data protection.

Note

Container services refer to AWS abstracting application containers behind the scenes, not Docker container services. This enables AWS to move the responsibility of managing that platform away from customers.

What Is the Customer Responsible For?

You're responsible for security in the cloud. When using any AWS service, you're responsible for properly configuring the service and your applications, as well as ensuring your data is secure.

The level of responsibility you have depends on the AWS service. Some services require you to perform all the necessary security configuration and management tasks, while other more abstracted services require you to only manage the data and control access to your resources. Using the three categories of AWS services, you can determine your level of responsibility for each AWS service you use.

Category	AWS Responsibility	Customer Responsibility
Infrastructure services	AWS manages the infrastructure and foundation services.	You control the operating system and application platform, as well as encrypting, protecting, and managing customer data.
Container services	AWS manages the infrastructure and foundation services, operating system, and application platform.	You are responsible for customer data, encrypting that data, and protecting it through network firewalls and backups.
Abstracted services	AWS operates the infrastructure layer, operating system, and platforms, as well as server-side encryption and data protection.	You are responsible for managing customer data and protecting it through client-side encryption.

Due to the varying level of effort, it's important to consider which AWS service you use and review the level of responsibility required to secure the service. It's also important to review how the shared security model aligns with the security standards in your IT environment, as well as any applicable laws and regulations.

It's important to note that you maintain complete control of your data and are responsible for managing the security related to your content. Here are some examples of your responsibilities in context.

- Choosing a Region for AWS resources in accordance with data sovereignty regulations
- Implementing data protection mechanisms, such as encryption and managing backups
- Using access control to limit who has access to your data and AWS resources

Resources

- External Site: AWS: Shared Responsibility Model