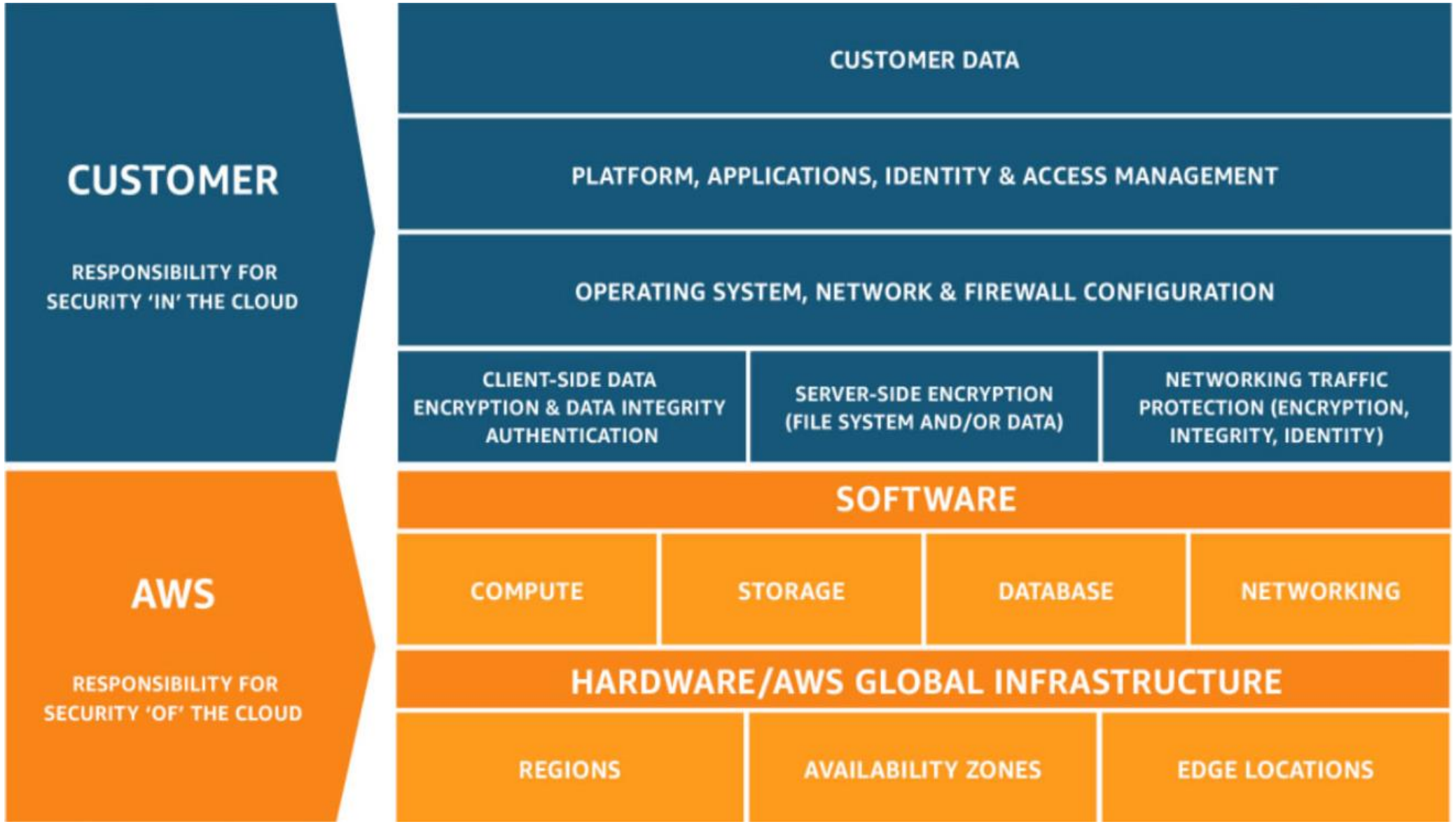
Shared Responsibility Model

Module 3


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
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
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

What is Shared Responsibility Model and How Does It Work?

- The shared responsibility model proposed by AWS is a scheme for allocating duties between AWS and a Customer.
- This means IN the cloud; security is not just the responsibility of the cloud service provider (CSP) for a business.
- Instead, the security OF the cloud-based deployment is a shared responsibility between the cloud provider and the cloud client, and the cloud provider's shared responsibility model explains the duties of each side.
- The infrastructure that powers all of the services provided by the AWS Cloud is under the control of AWS.
- The facilities, networking, hardware, and software used to run AWS Cloud services make up this infrastructure.
- The AWS Cloud services a client chooses will define the extent of the customer's obligation.
- The quantity of setup work the client must complete as part of their security obligations is determined by this.

Security in the cloud :

- This usually consists of the data that is uploaded/added by the customer.
- This data can be things like **names for the resources** that are being created, **the files that belong to the customer** which they upload .
- The customer is responsible for managing the data that he/she uploads.
- Next, coming to the types of configurations(Network and Firewall)that are chosen to maintain security is again something that the customer is held responsible for.
- Let's say if a user creates an EC2 instance, they themselves are responsible for the type of configurations that they are doing and are also responsible for the management of the Operating System that is being used on the created EC2 instance.
- Here, the management tasks can be looking after updates and security patches and configuration tasks can be things like creating rules on the security firewall to avoid malicious user access.

Security of the cloud :

- In this case, AWS takes the sole responsibility of keeping the customer created infrastructure secure.
- Here, "**Infrastructure**" are things like the compute, storage, software and networking based resources that runs on AWS.

Shared responsibility between AWS and the customer

- 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.

AWS responsibility “Security of the Cloud”

- AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.
- This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility “Security in the Cloud”

- Customer responsibility will be determined by the AWS Cloud services that a customer selects.
- This determines the amount of configuration work the customer must perform as part of their security responsibilities.
- For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Customer responsibility “Security in the Cloud”

- Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.
- For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.
- Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

- Inherited Controls – Controls which a customer fully inherits from AWS.
  - Physical and Environmental controls
- Customer Specific – Controls which 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.

Levels of Abstraction in Cloud

- There might not always be a common set of security responsibilities.
- Every circumstance can need a different level of security and responsibility.
- Degrees of abstraction are, thus, the area that pertains to such obligations. The terms "**levels of abstraction**" refer to PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and SaaS (Software as a Service).
- **Infrastructure as a Service (IaaS)**-The most basic level of abstraction is Infrastructure as a service. IaaS allows cloud suppliers to make their data centers' servers, storage, networks, hardware, and virtualization available to consumers.
- Although the user has much power, they also bear more security responsibility
- For example, if a user creates an **EC2 instance**, it is their responsibility to set up a security group to avoid access on certain ports. Therefore, here the user has the highest amount of responsibility to protect his EC2 instance.

Levels of Abstraction in Cloud

- **Platform as a Service (PaaS)** - The subsequent abstraction level enables users to create and consume apps. The cloud vendor also offers a platform for developing, deploying, and managing applications under **PaaS**, apart from the Infrastructure.
- **Software as a Service (SaaS)**-The cloud vendor hosts applications under SaaS to make them accessible to end-users or clients.
- Organizations no longer need to host programs in their own private data centers, thanks to SaaS. RDS (Relational Database Service) that provides a fully working relational DB service like SQL is an example of **SaaS in AWS**.
- Now coming to an example out of AWS, Adobe Photoshop is a SaaS that people use to edit their pictures.

Shared Security Responsibility Model			
On-Premises	IaaS	PaaS	SaaS
Users	Users	Users	Users
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network	Network	Network	Network
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility

Cloud Provider Responsibility

Shared Controls – Controls which 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 own control implementation within their use of AWS services.

Examples include:

- **Patch Management** – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- **Configuration Management** – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- **Awareness & Training** - AWS trains AWS employees, but a customer must train their own employees.

What is AWS Shared Responsibility Model?

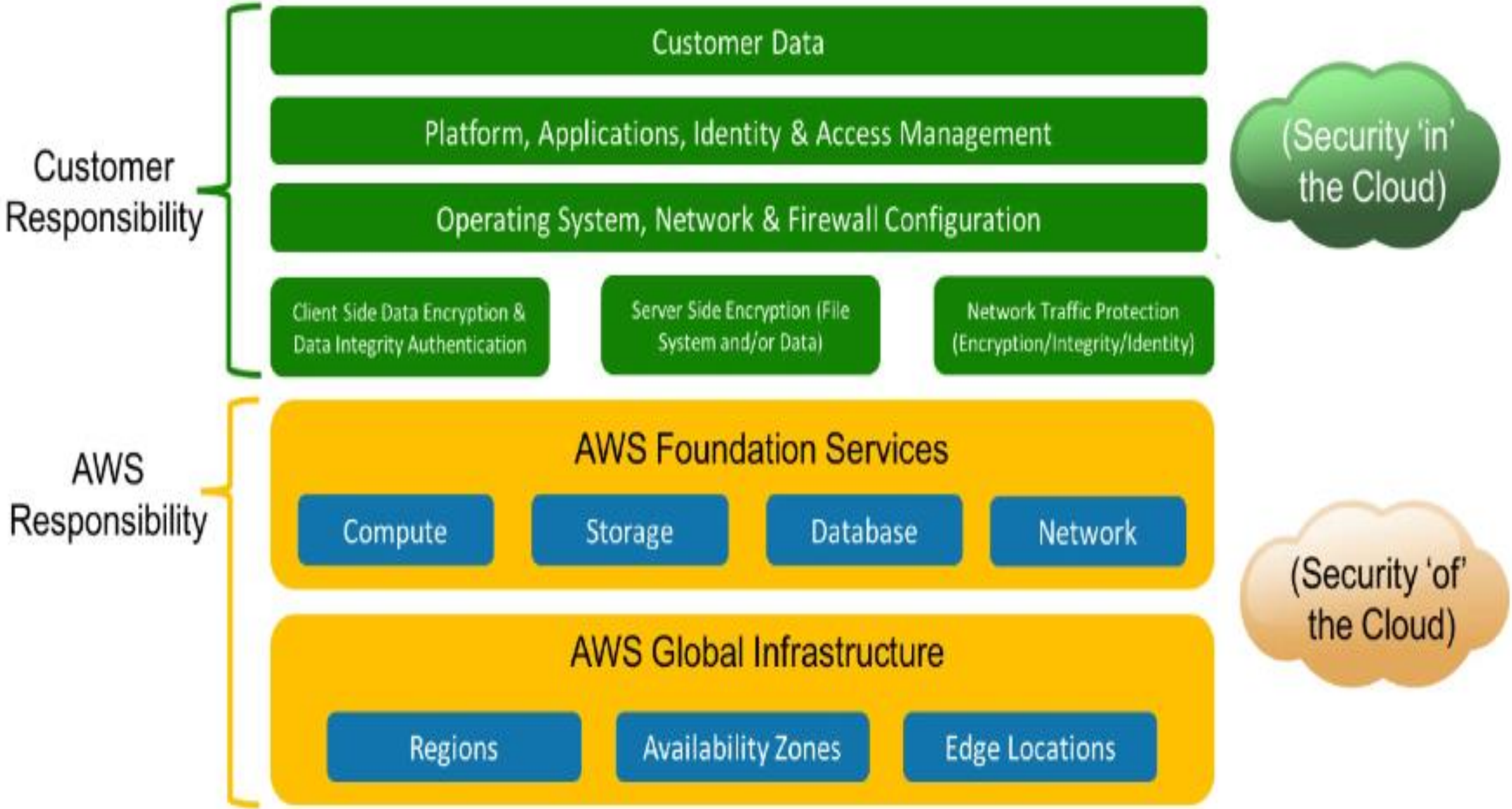
- **Responsibility of AWS**
- The Infrastructure that powers all of AWS's services must be kept secure.
- In other words, the components from the host operating system and virtualization layer down to the physical layer where the service is implemented are controlled, used, and managed by AWS.
- **Responsibility of a Customer**
- The client is responsible depending on the **AWS service** utilized and the settings required to protect it. In other words, guests' operating systems, security updates, and application software must be managed by customers.
- Additionally, users must set up the security measures supplied by AWS, such as security groups, network access control, and IAM (Identity and Access Management).

What is AWS Shared Responsibility Model?

- **Responsibility Differences**
- In addition to the infrastructure requirements of AWS, the user must supply their own control implementation in order to use AWS services:
- **IT controls**: AWS helps customers manage the burden of security measures including encryption, firewall upkeep, and deployments of IT controls in order to ensure proper adherence to **AWS security regulations**. AWS and its clients frequently share IT operations.
- **Configuration management**: While the client is responsible for configuring their own guest operating systems, databases, and software applications, AWS handles the configuration of its infrastructure equipment.
- AWS trains its personnel, but clients must also train their staff.

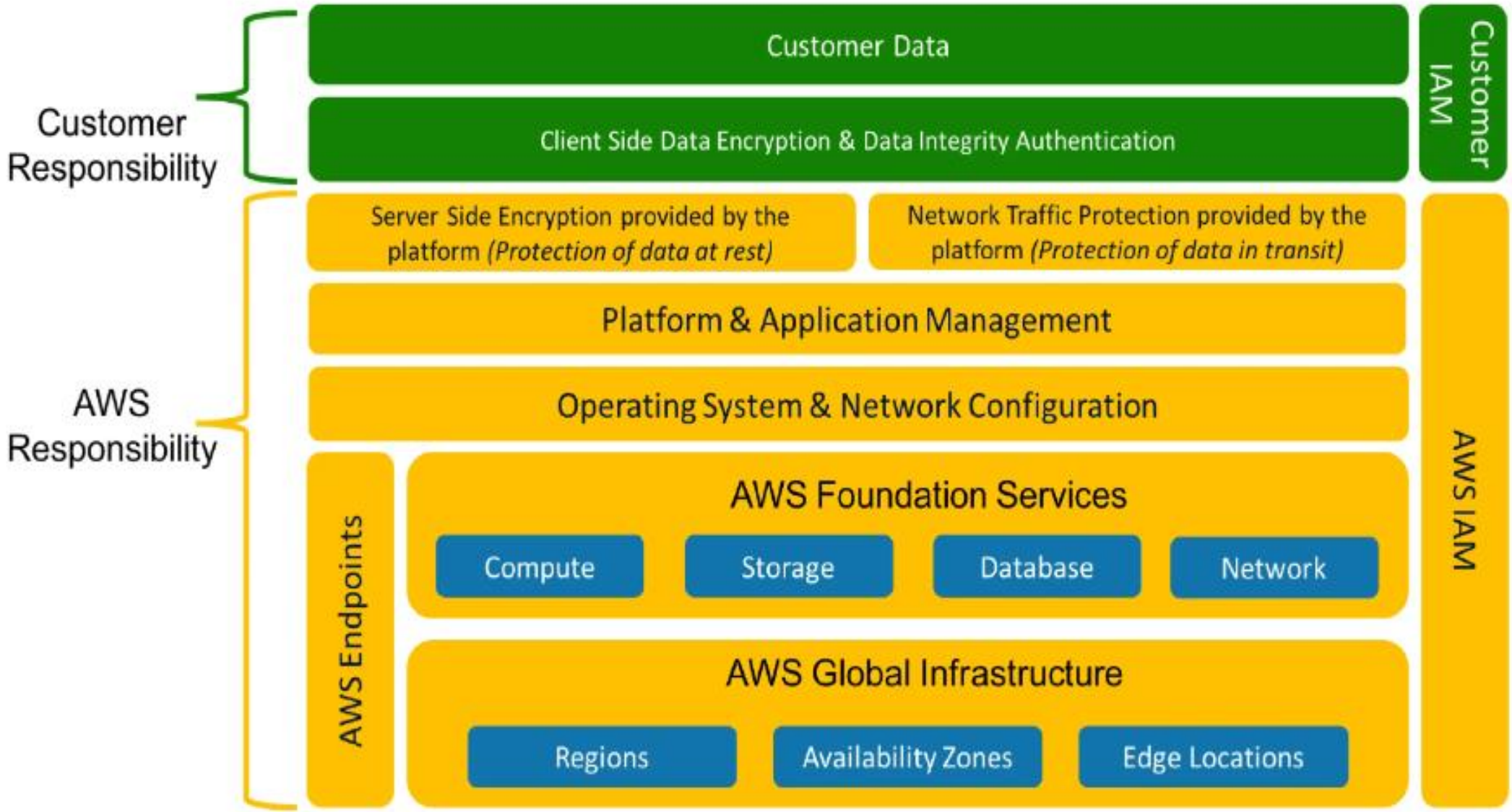
Types of AWS Shared Responsibility Model

- **AWS Shared Responsibility for Infrastructure Services**
- AWS is in charge of the security of the cloud. This includes the underpinnings of their compute, storage, database, and network services and its global infrastructure components, including regions, availability zones, and edge locations. Your client data is stored in data centers owned and controlled by AWS.
- This includes physical access to all hardware and networking parts and other data center amenities like generators, **UPS systems**, power distribution units (PDUs), computer room air conditioning (CRAC) units, and fire suppression systems. This physical access entry and control is the foundation for several security compliance procedures previously discussed. In essence, AWS is in charge of the elements that make up the cloud, and any data "inside" the cloud is your responsibility.
- You are in charge of what gets into the cloud since AWS is responsible for securing and maintaining the fundamental cloud infrastructure. This includes operating system security, network security, firewall setup, client and server-side encryption, network traffic protection, application security, and identity and access management.
- How much of this **additional protection** you choose to use is entirely up to you. Your choice can be affected by the nature of your business or by regulations currently in place. It's important to remember that even while AWS provides a number of reliable security measures, AWS is not in charge of deciding how and when to use them.


Customer Responsibility
Customer Data
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)
Network Traffic Protection (Encryption/Integrity/Identity)
(Security 'in' the Cloud)
AWS Responsibility
AWS Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
(Security 'of' the Cloud)

AWS Shared Responsibility for Container Services

- The consumer, in this instance, doesn't control their platform or operating system. A cloud customer's level of security responsibility is lower under this model than in the Infrastructure services. Their operating system is now out of sight and out of their hands. Therefore AWS is now in charge of it. According to this paradigm, the customer is principally in charge of firewall setting and adequately safeguarding their data (i.e., using encryption and access management).
- The administration of any operating system, system, or network configuration, as well as platform and application management, has been transferred to AWS and is no longer our duty as the client. In comparison to services dependent on Infrastructure, there is a significant distinction.
- Not all accountability has changed, though. You should be aware that platform and application management level integration does not affect firewall setup, which is still the end user's responsibility. For instance, you would be in charge of configuring and deploying security groups for Amazon RDS, the relational database service provided by AWS.


Customer Responsibility
AWS Responsibility
Customer Data
Client Side Data Encryption & Data Integrity Authentication
Customer IAM
Server Side Encryption provided by the platform (Protection of data at rest)
Network Traffic Protection provided by the platform (Protection of data in transit)
Platform & Application Management
Operating System & Network Configuration
AWS Endpoints
AWS Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS IAM

AWS Shared Responsibility for Abstract Services

- The security of the offered service must be appropriately configured, which is essentially the customer's responsibility. For instance, if a client sets up DynamoDB with user credentials that are simple to guess, they would be liable for any data breach.
- AWS will manage Network Traffic protection using the system that secures any information moving over the AWS network. You are also in charge of using IAM tools to apply the proper permissions at the platform level (S3 Bucket rules) and the IAM user/group level.
- The degree of control and accountability goes more toward AWS than the client as we move through these models.

Applying the AWS Shared Responsibility Model in Practice

- Once a customer understands the AWS Shared Responsibility Model and how it generally applies to operating in the cloud, they must determine how it applies to their use case.
- Customer responsibility varies based on many factors, including the AWS services and Regions they choose, the integration of those services into their IT environment, and the laws and regulations applicable to their organization and workload.

The following exercises can help customers in determining the distribution of responsibility based on specific use case:

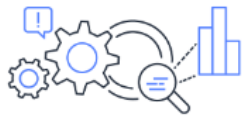
Determine external and internal security and related compliance requirements and objectives, and consider industry frameworks like the **NIST Cybersecurity Framework (CSF)** and **ISO**.

Consider employing the **AWS Cloud Adoption Framework (CAF)** and **Well-Architected best practices** to plan and execute your digital transformation at scale.

Review the security functionality and configuration options of individual AWS services within the security chapters of **AWS service documentation**.

Evaluate the **AWS Security, Identity, and Compliance services** to understand how they can be used to help meet your security and compliance objectives.

Review **third-party audit attestation documents** to determine inherited controls and what required controls may be remaining for you to implement in your environment.



Provide your internal and external audit teams with cloud-specific learning opportunities by leveraging the **Cloud Audit Academy** training programs.

Perform a **Well-Architected Review** of your AWS workloads to evaluate the implementation of best practices for security, reliability, and performance.

Explore solutions available in the **AWS Marketplace** digital catalog with thousands of software listings from independent software vendors that enable you to find, test, buy, and deploy software that runs on AWS.

Explore **AWS Security Competency Partners** offering expertise and proven customer success securing every stage of cloud adoption, from initial migration through ongoing day-to-day management.

- Thank you…

- Source: https://aws.amazon.com/compliance/shared-responsibility-model/