Shared Responsibility Model

Inherited controls

These are security controls the customer fully inherits from AWS. Perfect examples are the physical and environmental security controls used by Amazon.

Shared controls

These are controls that apply to both the infrastructure layer of Amazon and the customer responsibilities. Note that these shared controls apply to each domain in completely separate contexts or perspectives. AWS provides the requirements for the infrastructure, and then the client must provide their own control implementation within their use of the services. A great example is Identity and Access Management (IAM). The IAM service must be secured, meet regulatory compliance, and function as intended, whereas the customer should create well-crafted policies.

Customer-specific controls

These are security controls the customer is solely responsible for, and they vary based on the services the customer selects, of course. A great example would be when you apply specific patches to one of your operating systems on an EC2 instance.

CLIENT RESPONSIBILITIES

Remember, the client is considered responsible for security in the cloud. The specific services selected will cause variations in the client responsibilities. For example, if you are relying heavily on Simple Storage Service (S3) for storage, you will be responsible for knowledge and proper configuration of the security permissions for your resources. Another example would be if the client chooses to use EC2 and run an operating system like Windows Server 2016. The client is required to keep the operating system updated and patched and is also responsible for the application software they require on this guest operating system. The client is responsible for the appropriate security group configuration for the EC2 instance as well.