6.1. Networking and Content Delivery – Cloud Network, CDN, DNS Services,
Cloud Load Balancing.
6.2. Cloud security and compliance concepts
6.3. Shared Responsibility model
6.4. Cloud Watch, Cloud Formation, Cloud logs, Personal Health Dashboard.
6.5. Cloud messaging and notification service

Cloud Network

Cloud network is referred to a computer network that exists within or is part of a cloud computing infrastructure.
It is a computer network that provides network interconnectivity between cloud based or cloud enabled application, services and solutions. Cloud network can be cloud based network or cloud enabled network.

Cloud network primarily enables a cloud computing infrastructure / solution, its associated components and external users/ application /services to communicate with each other. Typically, cloud network works similar to a standard computer network but its components / devices / operations are centered on cloud computing.

For example, a cloud network will enable connecting a remote user with a cloud application (SaaS) or cloud infrastructure (IaaS). User queries from a web browser/ internet are delivered to and from the remote/backend cloud infrastructure. Similarly, cloud networks also enable the network communication between virtual machines.

CDN [Content Delivery Network]

A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content.

A CDN allows for the quick transfer of assets needed for loading Internet content including HTML pages, javascript files, stylesheets, images, and videos. The popularity of CDN services continues to grow, and today the majority of web traffic is served through CDNs, including traffic from major sites like Facebook, Netflix, and Amazon.

A properly configured CDN may also help protect websites against some common malicious attacks, such as Distributed Denial of Service (DDOS) attacks.

Is a CDN the same as a web host?

While a CDN does not host content and can't replace the need for proper web hosting, it does help cache content at the network edge, which improves website performance. Many websites struggle to have their performance needs met by traditional hosting services, which is why they opt for CDNs.

By utilizing caching to reduce hosting bandwidth, helping to prevent interruptions in service, and improving security, CDNs are a popular choice to relieve some of the major pain points that come with traditional web hosting.

What are the benefits of using a CDN?

Although the benefits of using a CDN vary depending on the size and needs of an Internet property, the primary benefits for most users can be broken down into 4 different components:

- **Improving website load times** - By distributing content closer to website visitors by using a nearby CDN server (among other optimizations), visitors experience faster page loading times. As visitors are more inclined to click away from a slow-loading site, a CDN can reduce bounce rates and increase the amount of time that people spend on the site. In other words, a faster a website means more visitors will stay and stick around longer.

- **Reducing bandwidth costs -** Bandwidth consumption costs for website hosting is a primary expense for websites. Through caching and other optimizations, CDNs are able to reduce the amount of data an origin server must provide, thus reducing hosting costs for website owners.

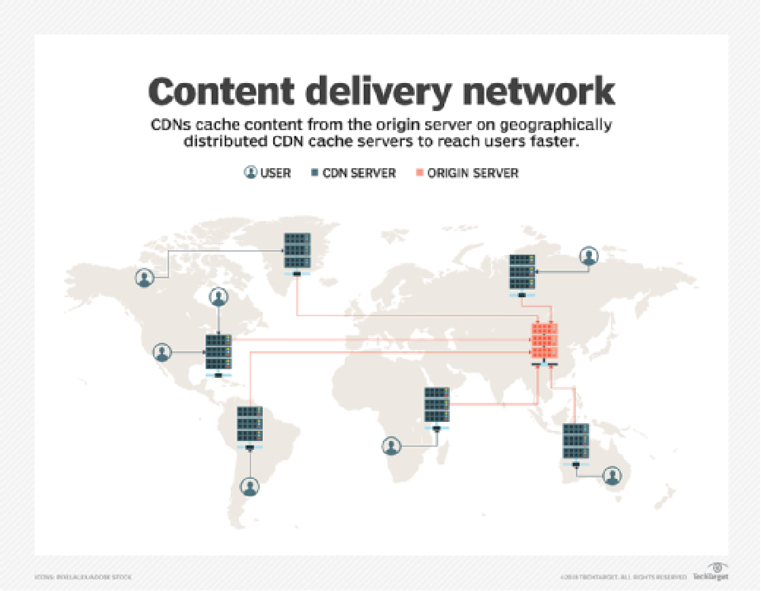
- **Increasing content availability and redundancy -** Large amounts of traffic or hardware failures can interrupt normal website function. Thanks to their distributed nature, a CDN can handle more traffic and withstand hardware failure better than many origin servers.

- **Improving website security -** A CDN may improve security by providing DDoS mitigation, improvements to security certificates, and other optimizations.

How does a CDN work?

At its core, a CDN is a network of servers linked together with the goal of delivering content as quickly, cheaply, reliably, and securely as possible. In order to improve speed and connectivity, a CDN will place servers at the exchange points between different networks.

These Internet exchange points (IXPs) are the primary locations where different Internet providers connect in order to provide each other access to traffic originating on their different networks. By having a connection to these high speed and highly interconnected locations, a CDN provider is able to reduce costs and transit times in high speed data delivery.

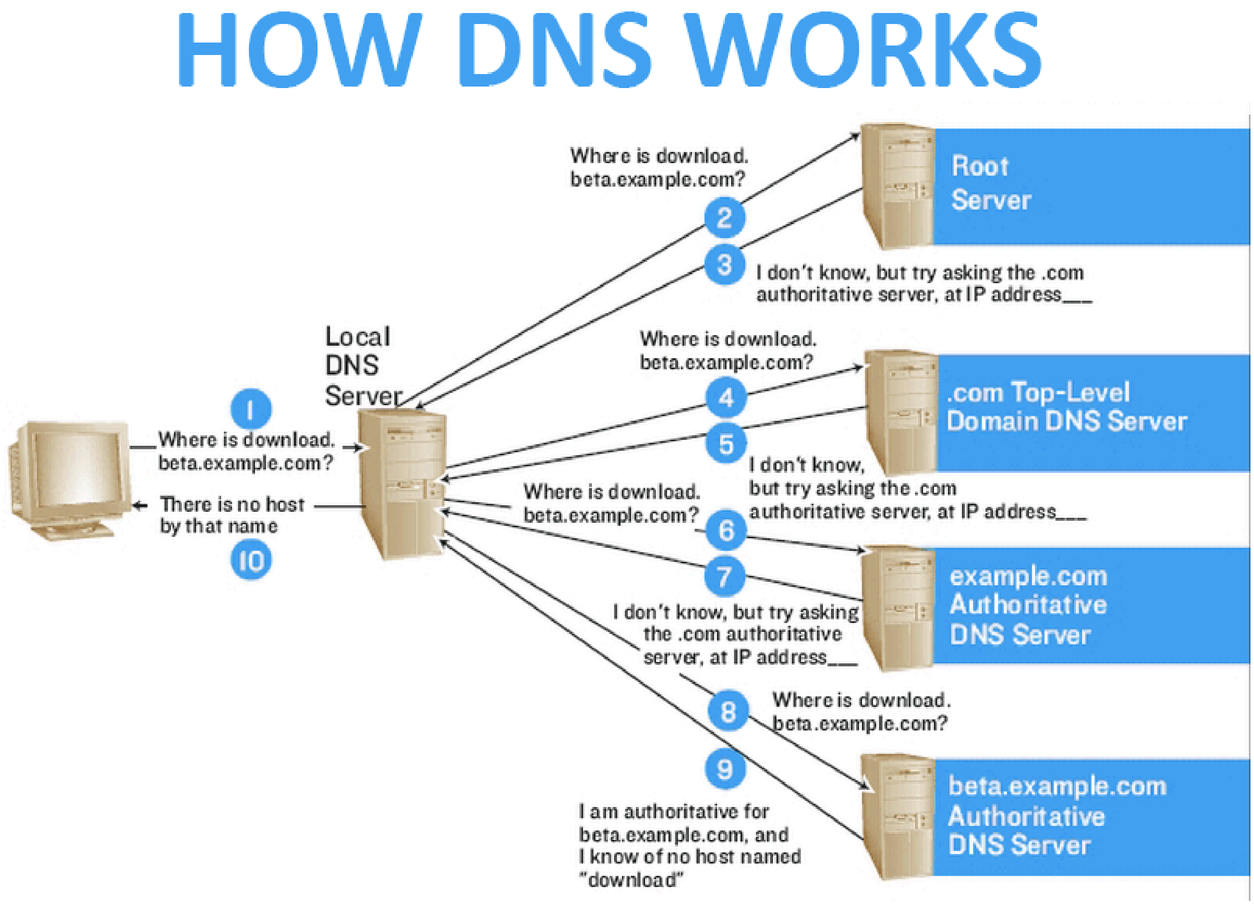

Content delivery network
CDNs cache content from the origin server on geographically distributed CDN cache servers to reach users faster.
USER
CDN SERVER
ORIGIN SERVER
ICONS: PIXELALEX/ADOBE STOCK
©2018 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Beyond placement of servers in IXPs, a CDN makes a number of optimizations on standard client/server data transfers. CDNs place Data Centers at strategic locations across the globe, enhance security, and are designed to survive various types of failures and Internet congestion.

DNS SERVICES

IT infrastructure isn't the only thing you can migrate from a legacy environment to Cloud Platform. Have you considered the impact of using legacy servers for hosting your domain name system (DNS) versus those of a cloud provider?

Domain name systems are hierarchical databases that store information to turn user-friendly domain names, such as onixnet.com, into numeric IP addresses.


HOW DNS WORKS
Where is download. beta.example.com?
2
3
Root Server
I don't know, but try asking the .com authoritative server, at IP address___
Local DNS Server
Where is download. beta.example.com?
4
5
.com Top-Level Domain DNS Server
I don't know, but try asking the .com authoritative server, at IP address___
1
Where is download. beta.example.com?
There is no host by that name
10
Where is download. beta.example.com?
6
7
example.com Authoritative DNS Server
I don't know, but try asking the .com authoritative server, at IP address___
8
Where is download. beta.example.com?
9
beta.example.com Authoritative DNS Server
I am authoritative for beta.example.com, and I know of no host named "download"

Cloud DNS provides users with a high-performance, resilient and global DNS service that makes it easier to manage your applications while giving users easy access to these applications.

It all runs on Google Cloud’s trusted infrastructure rather than your on-premise or hosted data center server and provides you with easy lookup of your authoritative name servers.

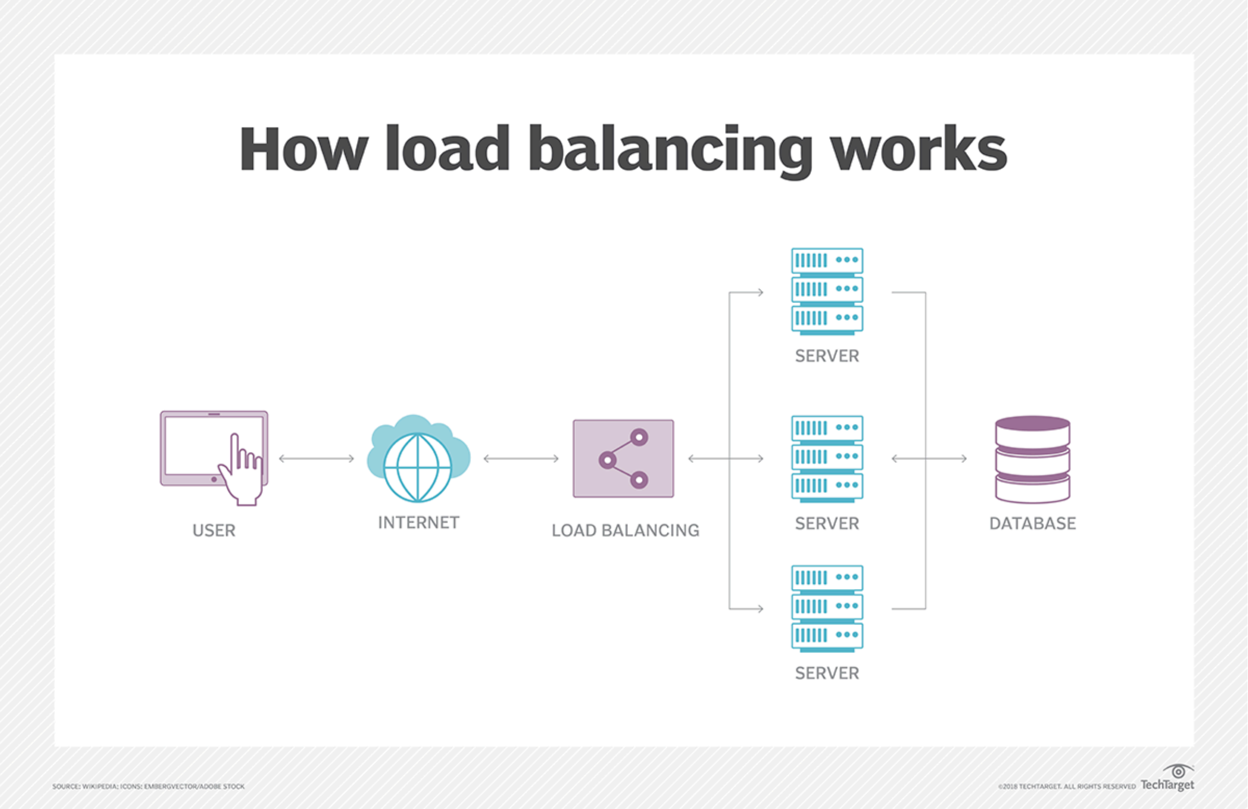
In more technical terms, as described by Google Cloud, Cloud DNS “acts as an authoritative DNS server for public zones that are visible to the internet, or for private zones that are visible only within your network.” Each zone is a container of DNS records and allows for more granular, administrative control of DNS components

Cloud Load Balancing

Cloud load balancing is the process of distributing workloads across computing resources in a cloud computing environment and carefully balancing the network traffic accessing those resources. Load balancing enables organizations to meet workload demands by routing incoming traffic to multiple servers, networks or other resources, while improving performance and protecting against disruptions in services. Load balancing also makes it possible to distribute workloads across two or more geographic regions.

Cloud load balancing helps enterprises achieve high performance levels for potentially lower costs than traditional on-premises load balancing technology. Cloud load balancing takes advantage of the cloud's scalability and agility to meet the demands of distributed workloads with high numbers of client connections. It also improves overall availability, increases throughput and reduces latency.

In addition to workload and traffic distribution, cloud load balancing services typically offer other features, such as application health checks, automatic scaling and failover and integrated certificate management.



SOURCE: WIKIPEDIA; ICONS: EMBERGVECTOR/ADOBE STOCK

©2018 TECHTARGET. ALL RIGHTS RESERVED

Cloud load balancing takes a software-based approach to distributing network traffic across resources, as opposed to hardware-based load balancing, which is more common in enterprise data centers. A load balancer receives incoming traffic and routes those requests to active targets based on a configured policy. A load balancing service also monitors the health of the individual targets to ensure that those resources are fully operational.

Examples of cloud load balancing services

Many cloud providers offer load balancing services, including the three major platforms:

- Amazon Web Services (AWS) Elastic Load Balancing distributes incoming client traffic and routes it to registered targets such as EC2 instances. Elastic Load balancing supports four types of load balancers: Application, Network, Gateway and Classic. The load balancers differ in the features offered, the network layers at which they operate and supported communication protocols.

- The Cloud Load Balancing service available on Google Cloud Platform is built on the same front-end server infrastructure that powers Google. The service offers a range of load balancers that vary depending on whether the customer needs external or internal load balancing, global or regional load balancing, Premium or Standard network service tiers, proxy or pass-through services, among other factors.
- Microsoft Azure offers four load balancing services. Azure Traffic Manager is a (OSI model) layer 7 DNS-based traffic load balancer for delivering services across global Azure regions. Azure Load Balancer is a layer 4 network load balancer for routing traffic between VMs. Azure Application Gateway is a layer 7 delivery controller for regional applications. Azure Front Door is a highly secure, layer 7 global load balancer for microservice.

Cloud Compliance

Cloud storage and SaaS solutions bring unprecedented speed, agility, and flexibility to a business. However, trusting third-party vendors with sensitive data comes with numerous inherent risks, such as:

- Insecure access points can increase the likelihood of breaches.
- Cloud services introduce multiple changes to traditional identity and access management (IAM) practices.
- Trusting a vendor with your sensitive data makes you reliant on their security practices.
- Your data becomes more vulnerable to natural disasters, DDoS attacks, and hijacking.
- There is a lack of visibility and control of your data.

Cloud deployments deliver accessibility, but they also create open, decentralized networks with increased vulnerability. This is where cloud compliance frameworks come in. **Aligning your data security policies and procedures to cloud compliance frameworks can help you mitigate the risks of deploying third-party cloud infrastructure and SaaS solutions.**

Key Components of a Cloud Compliance Framework

Governance

These preset controls protect your sensitive data from dangerous public exposure. Essential areas of cloud governance include:

- Asset management involves organizations taking stock of all cloud services and data contained, then defining all configurations to prevent vulnerability.
- Cloud strategy and architecture includes characterizing cloud structure, ownership, and responsibilities in addition to integrating cloud security.
- Financial controls address a process for authorizing cloud service purchases and balancing cloud usage with cost-efficiency

Change Control

Two of the cloud's biggest advantages, speed and flexibility, make controlling change more difficult. Inadequate change control often results in problematic misconfigurations in the cloud. Organizations should consider leveraging automation to continuously check cloud configurations for issues and ensure successful change processes.

Identity and access management (IAM) controls often experience multiple changes in the cloud. A few IAM best practices:

- Continuously monitor root accounts, as they can allow dangerous unrestricted access. Disable them if possible or monitor with filters and alarms and require multi-factor authentication (MFA).
- Utilize role-based access and group level privileges, granting access based on business needs and the least privilege principle.
- Disable dormant accounts and institutionalize effective credential and key management policies.

Continuous Monitoring

The complexity and dispersed nature of the cloud make monitoring and logging all activity extremely important. Capturing the who, what, when, where, and how of events keeps organizations audit-ready and is the backbone of compliance verification. When monitoring and logging data in your cloud environment, it’s essential to:

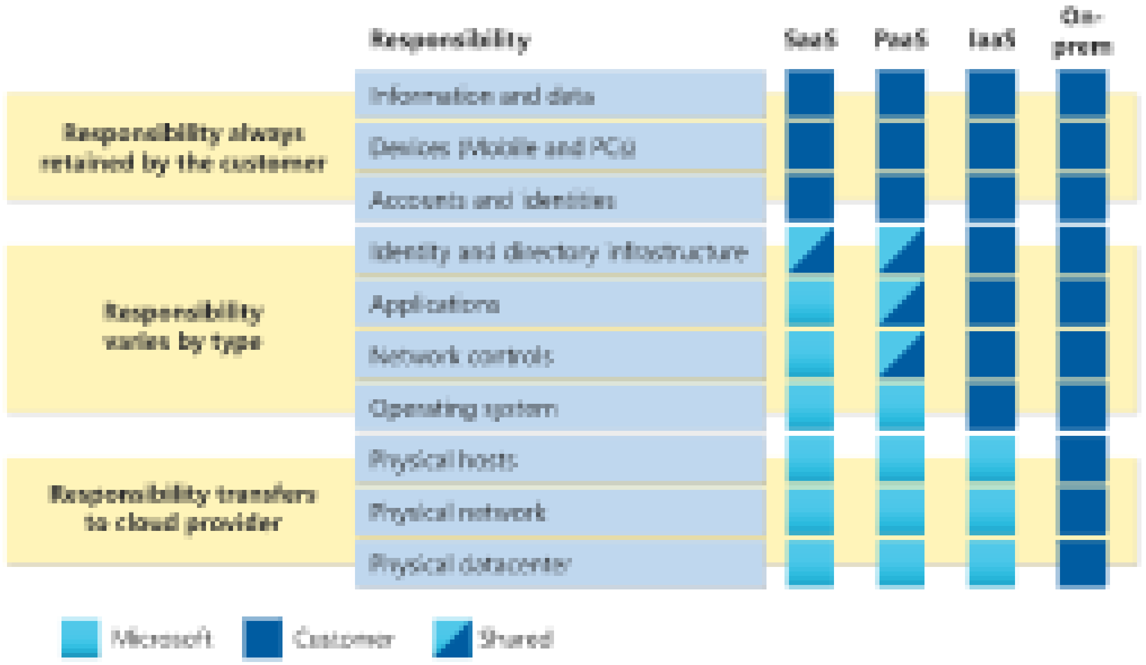
- Remember to enable logging all cloud resources
- Protect logs with encryption and don’t hold in public-facing storage
- Define your metrics and alarms, and record all activity
- Vulnerability Management

Reporting

Reporting provides current and historical proof of compliance. Think of these reports as your compliance footprint and very handy come audit time. A complete timeline of all events before and after an incident can provide critical evidence should your compliance ever be questioned.

Shared Responsibility Model (SRM)

Link:
https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Cloud adoption has accelerated in the past year as organizations scrambled to support a remote workforce. Despite this rapid adoption and growth, companies often misunderstand a key cloud concept: the shared responsibility model (SRM).

Many business leaders still ask, “Is the cloud secure”? This is the wrong question. A more appropriate question would be, “Are we, as a security team and organization, securing our share of the cloud?” The overwhelming majority of cloud data breaches/leaks are due to the customer, with Gartner predicting that through 2025, 99% of cloud security failures will be the customer's fault. For this reason, it is imperative that all security practitioners understand their responsibilities.

What is the shared responsibility model?

The shared responsibility model delineates what you, the cloud customer is responsible for, and what your cloud service provider (CSP) is responsible for. The CSP is responsible for security “of” the cloud—think physical facilities, utilities, cables, hardware, etc. The customer is responsible for security “in” the cloud—meaning network controls, identity and access management, application configurations, and data.

That said, this division of responsibilities can change depending on what service model you use. At a basic level, the NIST Definition of Cloud Computing defines three primary cloud service models:

- Infrastructure as a service (IaaS): Under the IaaS model, the CSP is responsible for the physical data center, physical networking, and physical servers/hosting.

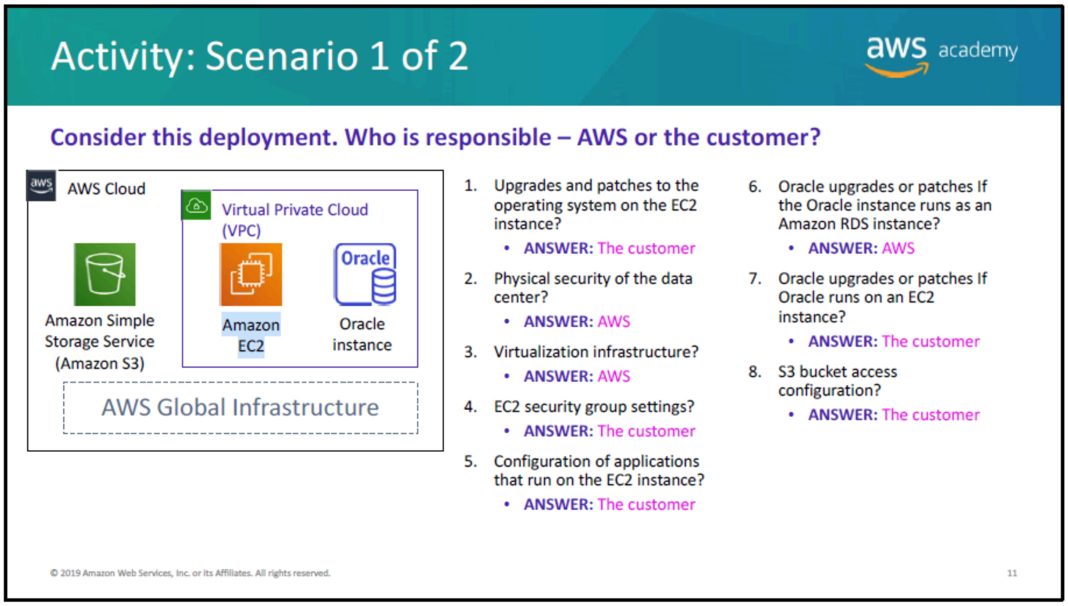
- Platform as a service (Paas): In a PaaS model, the CSP takes on more responsibility for things such as patching (which customers are historically terrible at and serves as a primary pathway to security incidents) and maintaining operating systems.

- Software as a service (SaaS): In SaaS, the customer can only make changes within an application's configuration settings, with the control of everything else being left to the CSP (think of Gmail a basic example)

Each comes with a tradeoff, with the customer relinquishing control in exchange for more of a turnkey/managed experience with the CSP handling more of the operational activities and letting the customer focus on their core competencies.

Look to your CSP for security resources. Amazon Web Services (AWS), for example, offers an incredible database of security documentation, broken down by categories (e.g., compute, storage, security, identity, and compliance) where you can find specifics associated with each of the services your organization is using. This includes myriad information from how to securely configure the services, what configurations you can manipulate, and troubleshooting guidance.

***Shared Responsibility**



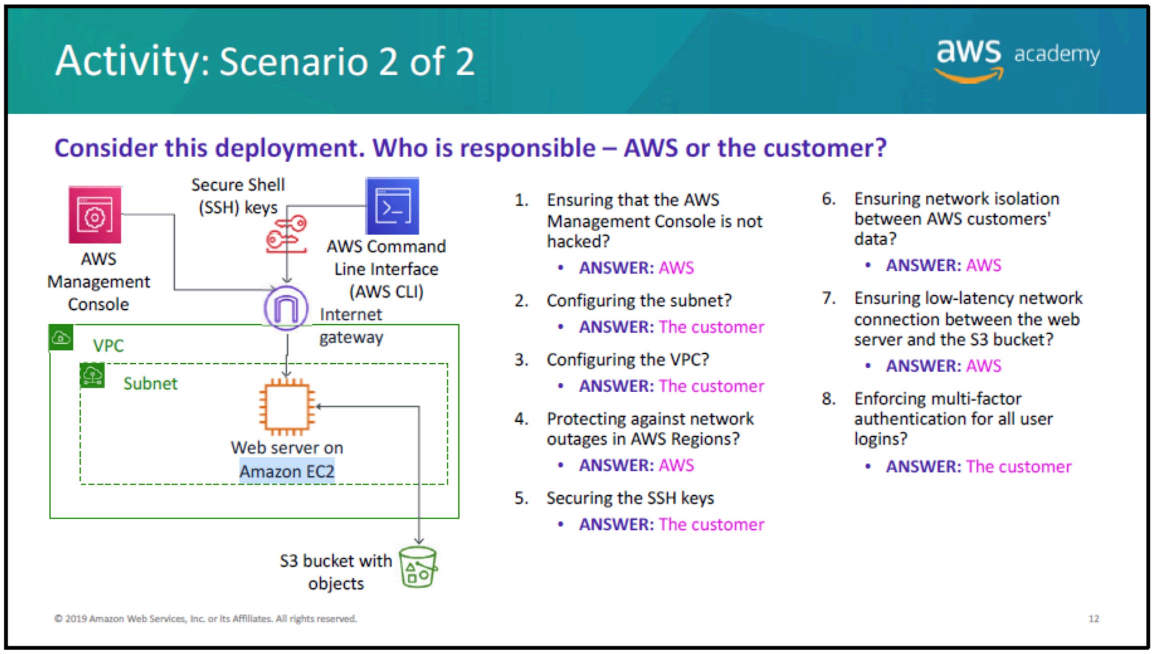
Activity: Scenario 1 of 2

aws academy

Consider this deployment. Who is responsible – AWS or the customer?

AWS Cloud
Virtual Private Cloud (VPC)
Amazon Simple Storage Service (Amazon S3)
Amazon EC2
Oracle
Oracle instance
AWS Global Infrastructure

1. Upgrades and patches to the operating system on the EC2 instance?
   - **ANSWER:** The customer
2. Physical security of the data center?
   - **ANSWER:** AWS
3. Virtualization infrastructure?
   - **ANSWER:** AWS
4. EC2 security group settings?
   - **ANSWER:** The customer
5. Configuration of applications that run on the EC2 instance?
   - **ANSWER:** The customer
6. Oracle upgrades or patches If the Oracle instance runs as an Amazon RDS instance?
   - **ANSWER:** AWS
7. Oracle upgrades or patches If Oracle runs on an EC2 instance?
   - **ANSWER:** The customer
8. S3 bucket access configuration?
   - **ANSWER:** The customer



Activity: Scenario 2 of 2

aws academy

Consider this deployment. Who is responsible – AWS or the customer?

Secure Shell (SSH) keys
AWS Management Console
AWS Command Line Interface (AWS CLI)
Internet gateway
VPC
Subnet
Web server on Amazon EC2
S3 bucket with objects

1. Ensuring that the AWS Management Console is not hacked?
   - **ANSWER:** AWS
2. Configuring the subnet?
   - **ANSWER:** The customer
3. Configuring the VPC?
   - **ANSWER:** The customer
4. Protecting against network outages in AWS Regions?
   - **ANSWER:** AWS
5. Securing the SSH keys
   - **ANSWER:** The customer
6. Ensuring network isolation between AWS customers' data?
   - **ANSWER:** AWS
7. Ensuring low-latency network connection between the web server and the S3 bucket?
   - **ANSWER:** AWS
8. Enforcing multi-factor authentication for all user logins?
   - **ANSWER:** The customer