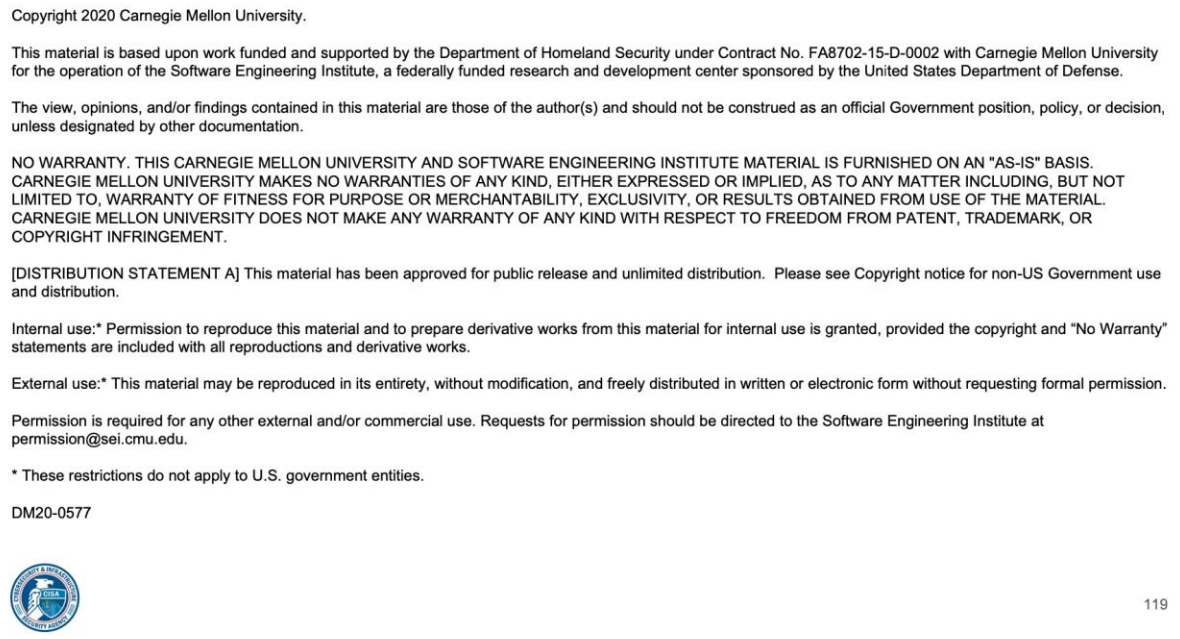
Cloud Computing Overview

Table of Contents

Notices



This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM20-0577

**001 Instructor: NIST Special Publication

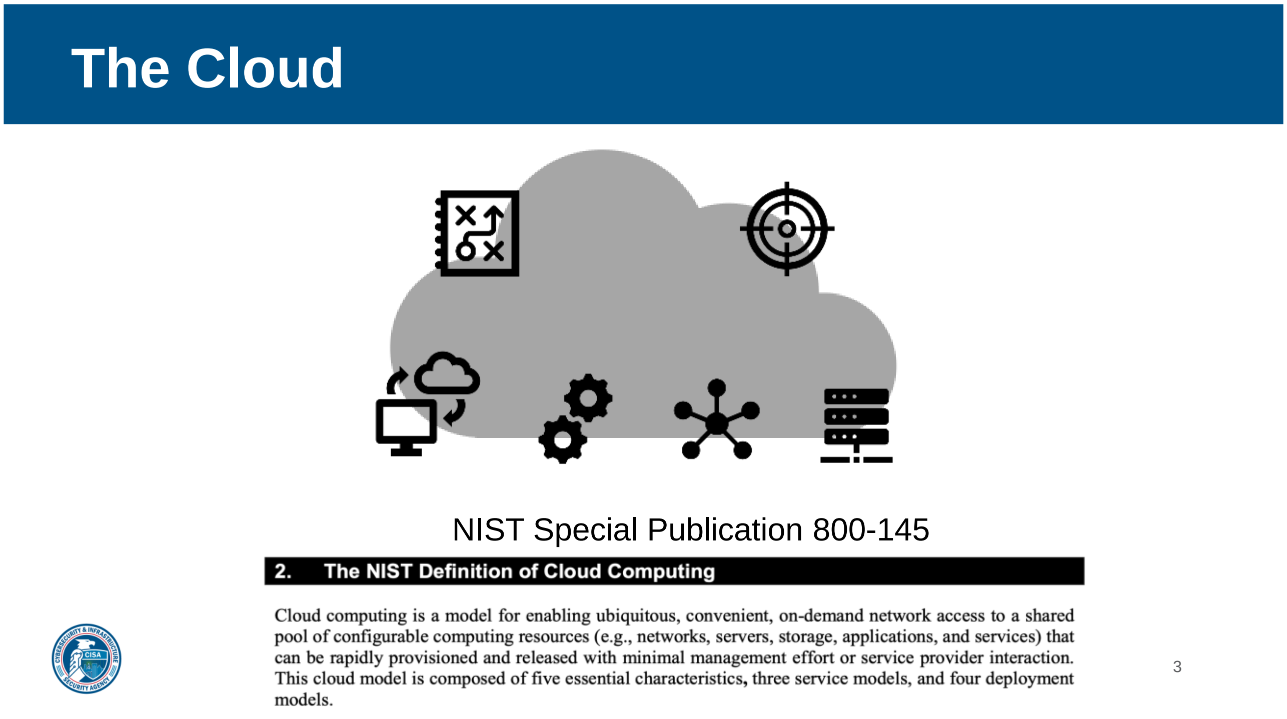
Cloud Computing Overview

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CLOUD COMPUTING OVERVIEW

**002 800-1145 defines cloud computing

The Cloud



The Cloud

NIST Special Publication 800-145

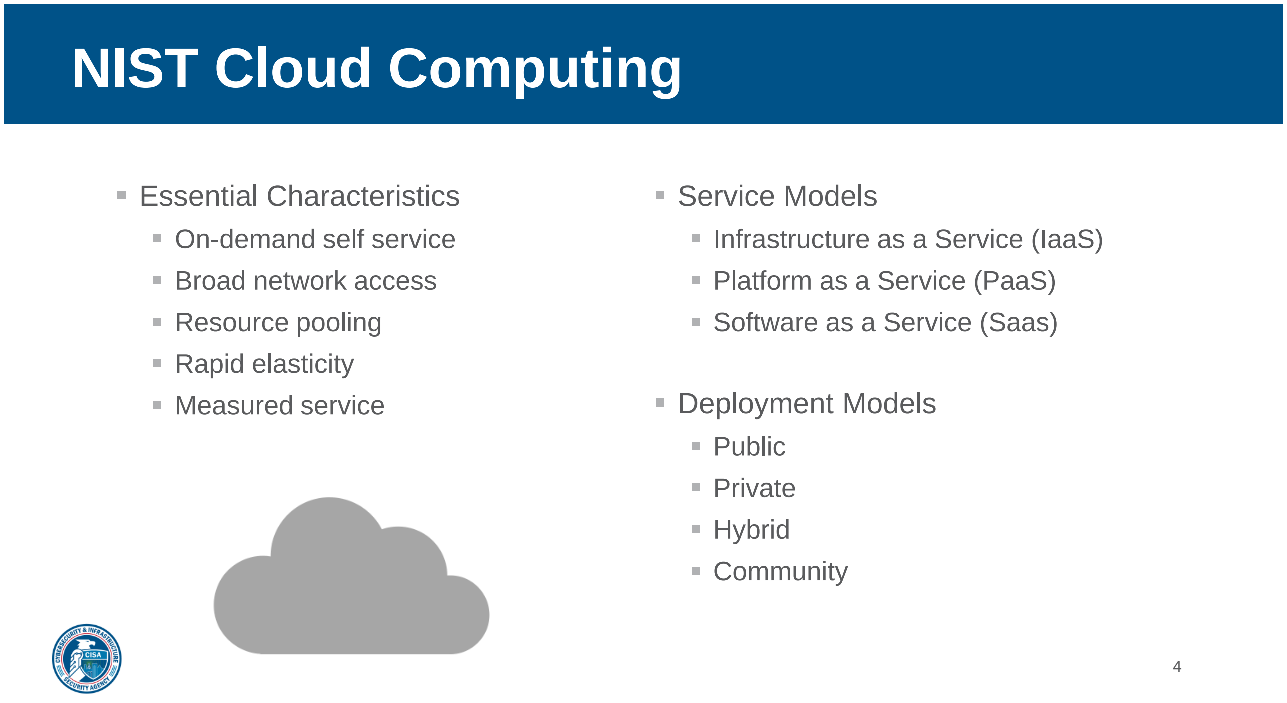
2. The NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

3

**003 but the term "cloud" may actually have several origins. One of the easiest comparisons is that the cloud is simply a metaphor for the internet, and a cloud has been used to symbolize the internet and/or diagrams for years. Cloud computing is an operational model that combines the benefits of virtualization and automation for new ways of delivering and consuming technology. The use of virtualization technologies allows the abstraction of resources from their underlying physical infrastructure and is what facilitates the creation of resource pools that maximize the use of underlying hardware. Rapid provisioning and de-provisioning of resources using automated methods such as scripts and applications is known as orchestration. This on-demand elasticity is one of the key differentiators between cloud and traditional virtualization solutions.

NIST Cloud Computing



NIST Cloud Computing

- Essential Characteristics
  - On-demand self service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

- Service Models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (Saas)

- Deployment Models
  - Public
  - Private
  - Hybrid
  - Community

4

**004 The five key characteristics of cloud computing as per NIST Special Pub 800-145 are on-demand self-service; broad network access; the ability to share pools of resources such as processing power, memory, and storage; the ability to shrink and grow rapidly based on demand; and finally, the ability to monitor and report on utilization for billing and performance metrics.

Broad network access is a bit more than fast internet connectivity, but also requires access to be available from standard clients such as desktops, laptops and mobile devices.

Measured service is the ability to automatically control and optimize resource usage and essentially pay for what you actually use.

Under Service Models, we have infrastructure as a service. Similar to on-premise virtualization, the customer is still responsible for all aspects of the solution, including the installation, configuration, and securing of the operating system, storage, applications and data. The cloud service provider is essentially providing the hosting facility, such as space, power, and network, along with the underlying hardware to support the solution.

Platform as a service further abstracts the underlying infrastructure from the customer. Maintenance tasks such as applying system patches are no longer required by the customer and the focus can be on securing the applications that are being developed.

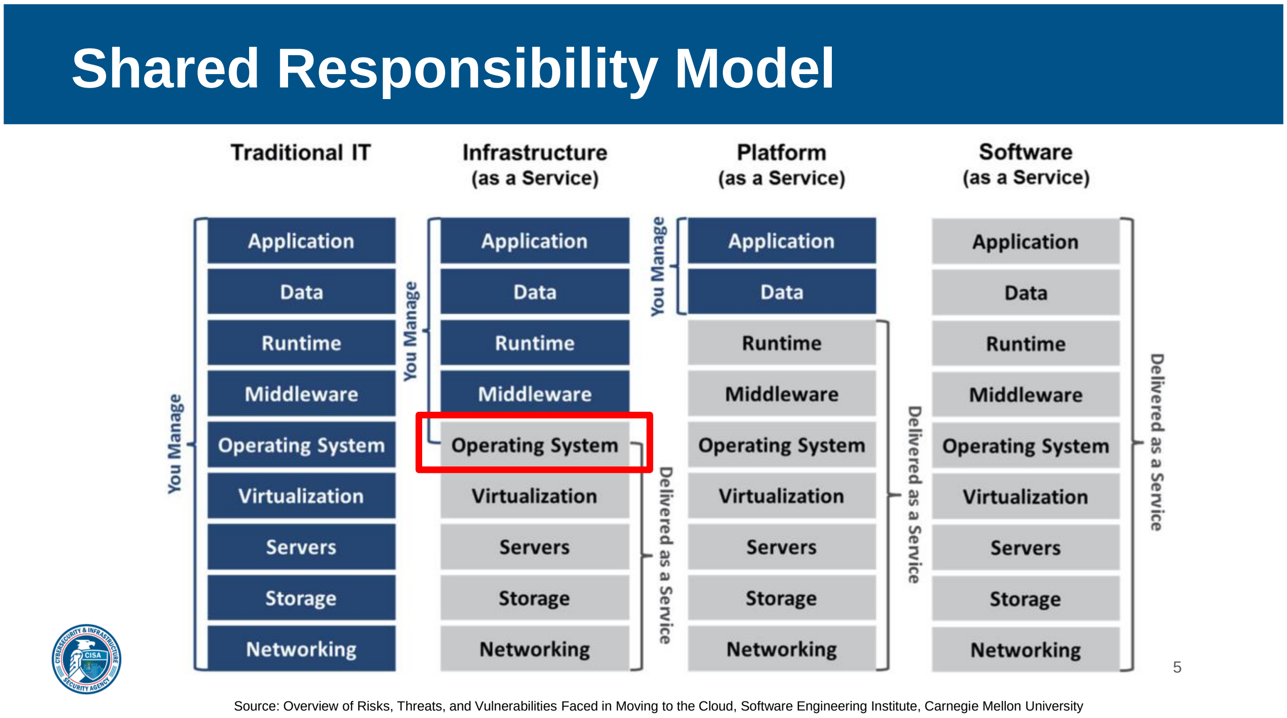
Essentially any internet-based application hosted by a third-party can be considered a platform as a service provided it meets the essential characteristics for elasticity, access, measured service, etc. Software as a service fully abstracts everything except the application itself. There are numerous examples of these, such as Salesforce, Gmail, Office 365, Dropbox, and the list goes on and on.

Deployment models describe how these are offered to consumers. Public clouds are open to anyone who signs up for the service. You can consider your favorite social media applications, like Twitter, Instagram, or Facebook to be public clouds, along with services like Google Cloud Platform, Microsoft Azure, and Amazon Web Services.

Private clouds are reserved only for trusted users. Although they can be operated by a single individual, their strengths include the ability to include and manage multiple users from an organization and assign permissions and usage privileges based on defined profiles. These can exist within public clouds like Azure and AWS. They can also be wholly owned and operated solutions built for and dedicated to a single organization.

Hybrid clouds connect on-premise resources to a public cloud deployment. There are now numerous ways to integrate and interoperate, including deployment of cloud agents to local enterprise servers, near-cloud storage solutions, and dedicated VPN tunnels to extend one network to the other.

Shared Responsibility Model



Shared Responsibility Model

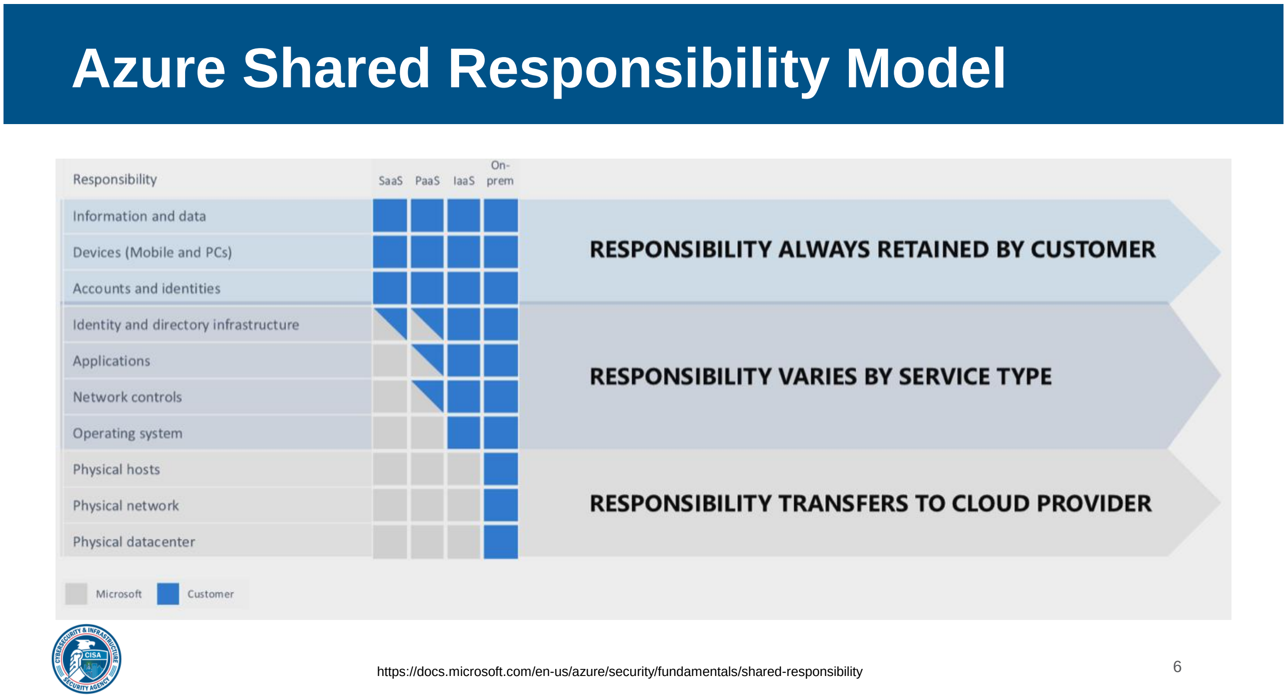
Traditional IT	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Application	Application	Application	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Source: Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud, Software Engineering Institute, Carnegie Mellon University

**005 Regardless of the service model, it is important to understand that access management, monitoring, log analysis, even configuration control are customer responsibilities. Your organization needs to define and implement strong password policies, consider multifactor authentication, and verify secure configurations are implemented.

Let's highlight this box here. In the Infrastructure as a service model, you see that both the customer and the provider have responsibility for securing in the OS. I would say the majority of this would fall on you. Even with configurable agents and services that help with monitoring and patch management, it is up to you to install and configure these. CSPs may have services and users that get automatically installed and configured to support APIs, so there's some expectation that this is done in a secure manner and in accordance with their published security standards. There are also underlying operating systems that provide the virtualization hypervisors, and protection of those host systems is always the responsibility of the cloud provider.

Azure Shared Responsibility Model



Azure Shared Responsibility Model

Responsibility	SaaS	PaaS	IaaS	On-prem	
Information and data	🟦	🟦	🟦	🟦	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦	
Accounts and identities	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	◩	◩	🟦	🟦	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	⬜	◩	🟦	🟦	
Network controls	⬜	◩	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Physical hosts	⬜	⬜	⬜	🟦	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER
Physical network	⬜	⬜	⬜	🟦	
Physical datacenter	⬜	⬜	⬜	🟦	

⬜ Microsoft 🟦 Customer

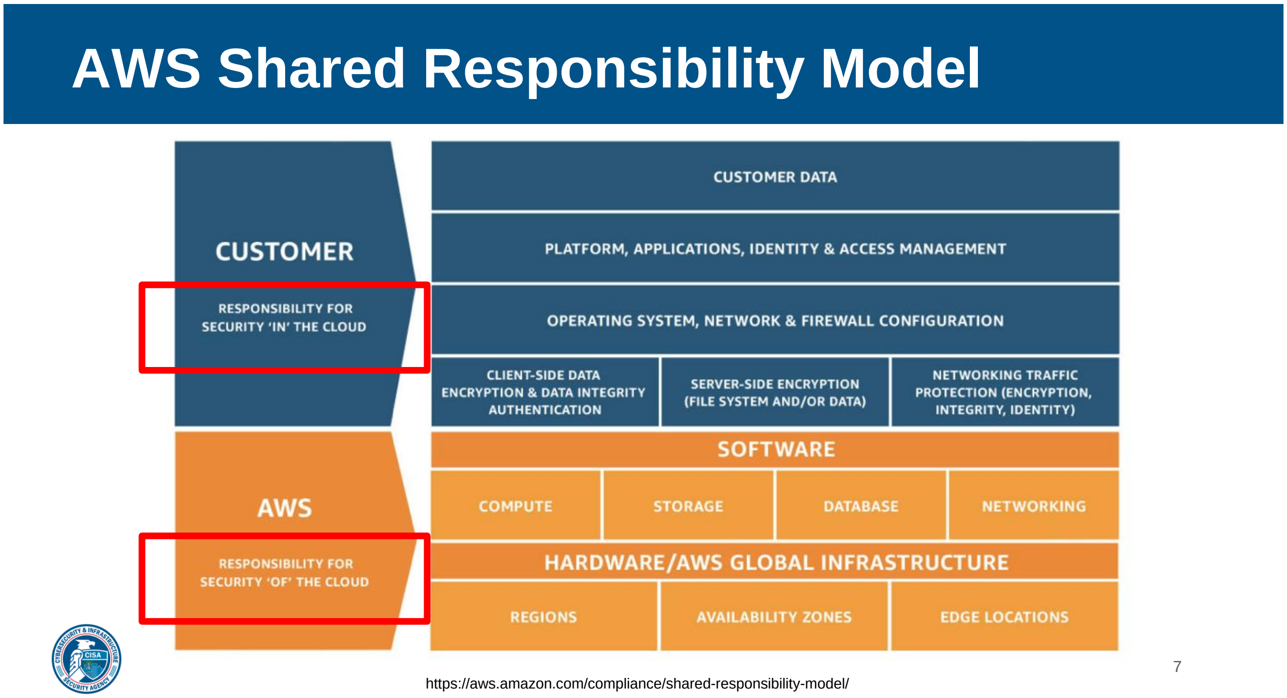
https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

6

**006 The Microsoft Azure Cloud Shared Responsibility Model is very similar to our previous example. Without going into too much detail here, note the underlying physical components are always the cloud provider's responsibility, and the upper-level elements related to users, data security and client devices are always the customer's responsibility;

and of course there's some variability based on the different services such as platform as a service, software as a service and infrastructure as a service.

AWS Shared Responsibility Model



AWS Shared Responsibility Model

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

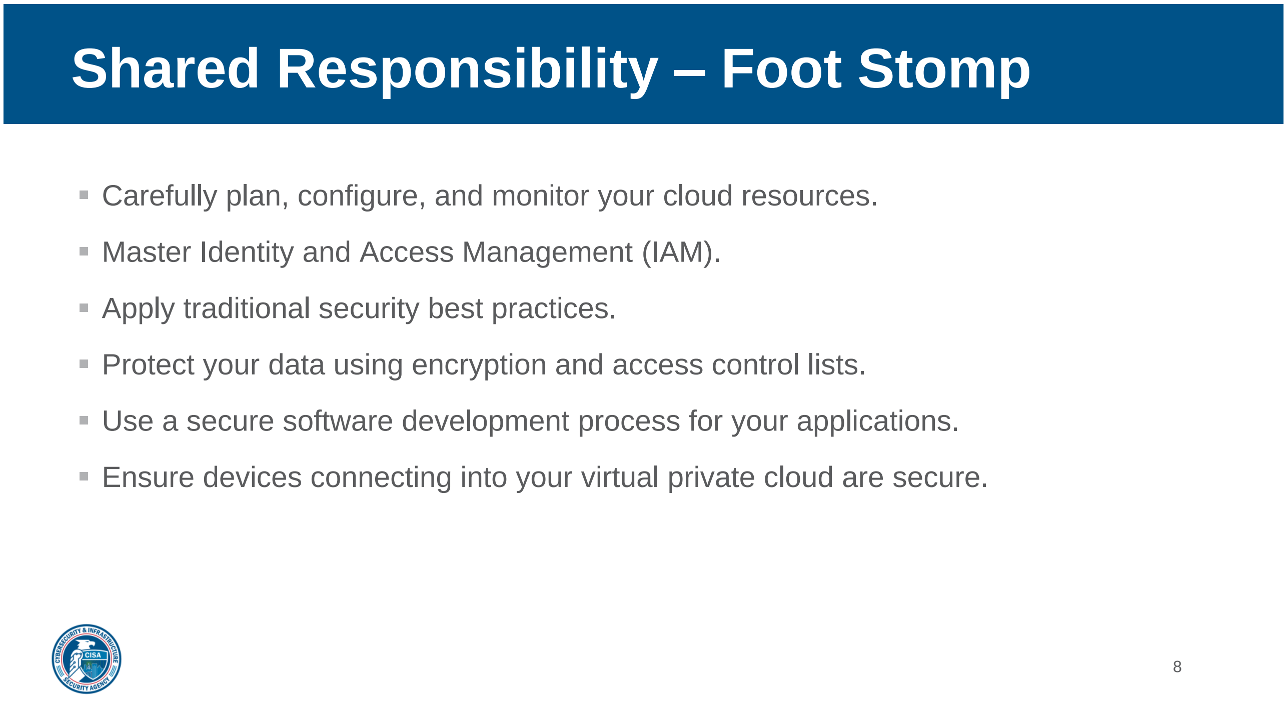
EDGE LOCATIONS

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

7

**007 If we take a look at Amazon's version of the shared responsibility model, we can see this presented in a similar manner, but right here is a great way to look at it. The cloud service provider-- in this case, Amazon-- is responsible for security of the cloud, meaning the hardware, software, networking, and facilities that make up their infrastructure. They are further responsible for ensuring the availability of services and proper segmentation and isolation in a multi-tenancy environment. The customer is responsible for security in the cloud, which includes proper configuration of the services, patching of the provisioned operating systems and applications, and protection of their own data.

Shared Responsibility – Foot Stomp



Shared Responsibility – Foot Stomp

- Carefully plan, configure, and monitor your cloud resources.
- Master Identity and Access Management (IAM).
- Apply traditional security best practices.
- Protect your data using encryption and access control lists.
- Use a secure software development process for your applications.
- Ensure devices connecting into your virtual private cloud are secure.

**008 So here's our foot stomp moment. When it comes to your cloud security responsibilities, your focus should be on the list here. Number one, properly configure identity and access management, especially the root or manager account for your cloud subscription. Next, apply traditional cybersecurity best practices. This includes implementing access control lists with default deny rules, implementing patch and configuration management programs, and enable logging, monitoring, and alert systems.

Admittedly, that one is fairly open-ended.

Data protection is next on our list, and this really means that you need to understand exactly what data your applications have access to, what are you storing, how are you protecting that information, and what regulations apply to that data set. Of course any application your organization is creating needs to leverage good software development practices, go through secure code reviews, vulnerability testing, etcetera. You don't want the bad guys finding a flaw before you do.

And the last one on our list is to ensure devices that connect into your cloud are secure. A compromised developer or admin machine could turn into your worst nightmare as it might open up the door to attackers

**009 for a plethora of attacks.