Cloud Service Adoption 101 - What You Need to Know

NTIA's Communications Supply Chain Risk Information Partnership

C-SCRIP Overview

- The Communications Supply Chain Risk Information Partnership (C-SCRIP) shares supply chain security risk information with trusted communications providers and suppliers.

- The target audience is small and rural companies in this sector, though larger companies and associations are not excluded from participating.

- Supply chain information comes from NTIA and other government partners, such as DHS/CISA, FBI, and the Intelligence Community.

- In addition to supply chain risk information, C-SCRIP shares trainings and webinars as well as grant opportunities.

Basics: Essential Characteristic of the Cloud
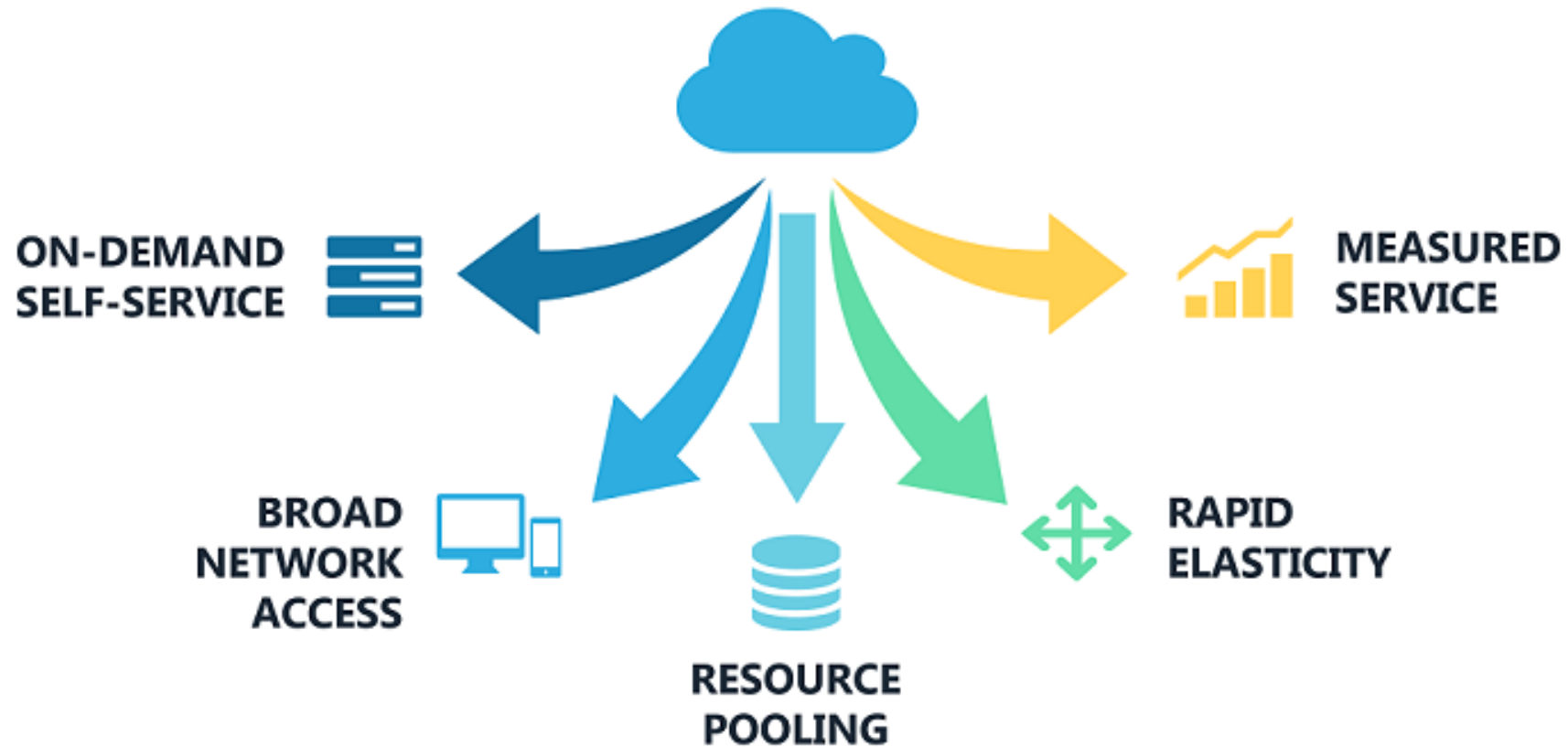
Source: GSA

Basics: Cloud Deployment Models

PUBLIC CLOUD   PRIVATE CLOUD   COMMUNITY CLOUD   HYBRID CLOUD
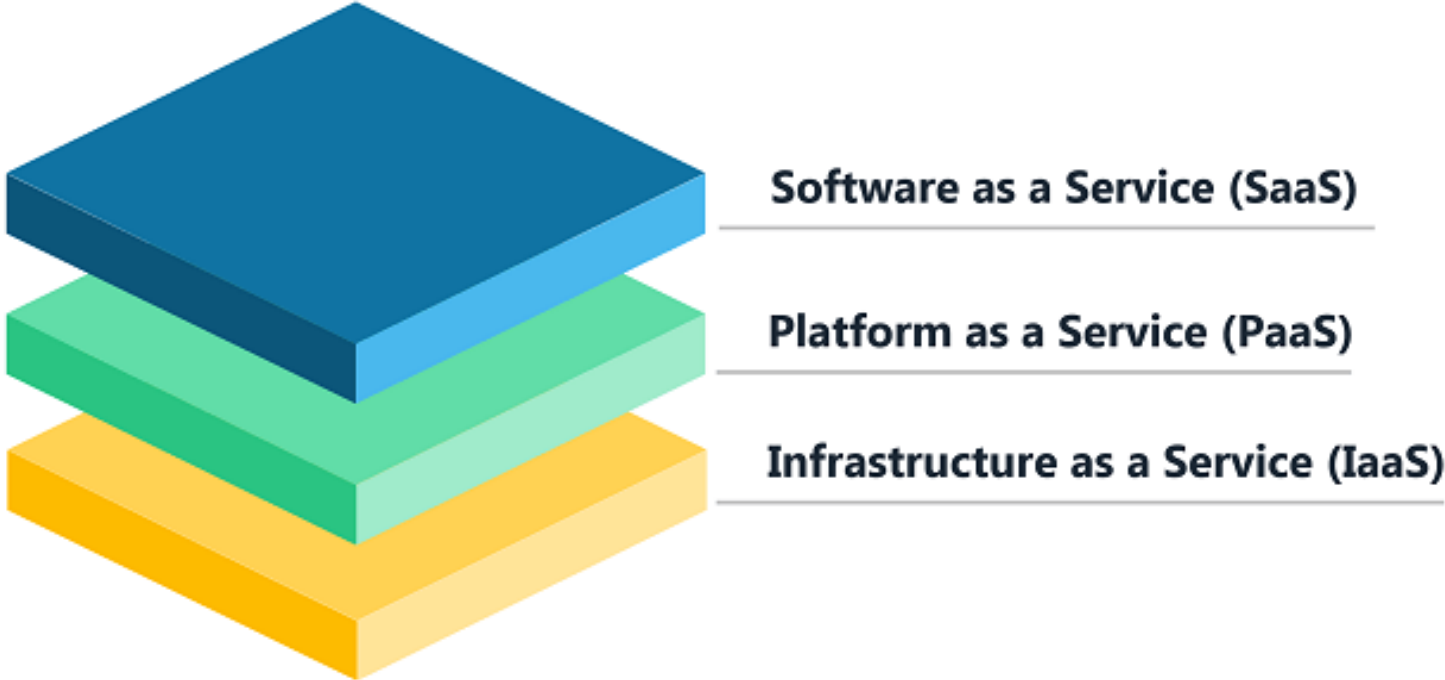
Source: GSA

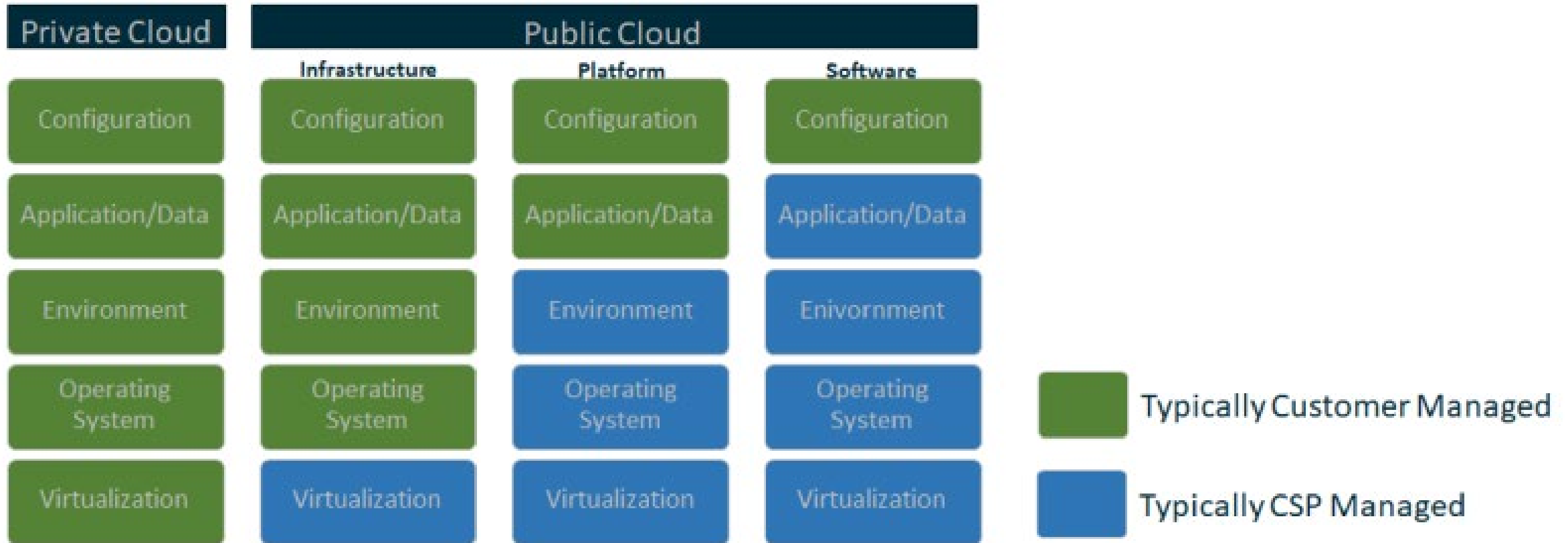# Basics: Cloud Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Source: GSA

Cloud Security: Shared Responsibility Model

Private Cloud	Public Cloud		
	Infrastructure	Platform	Software
Configuration	Configuration	Configuration	Configuration
Application/Data	Application/Data	Application/Data	Application/Data
Environment	Environment	Environment	Enivronment
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization

Typically Customer Managed

Typically CSP Managed

Source: NSA

Cloud Security: Considerations

1. **Threat Detection**

   1. CSPs are generally responsible for detecting threats to the underlying cloud platform, customers bear the responsibility of detecting threats to their own cloud resources.

2. **Incident Response**

   1. Incidents internal to customer cloud environments are generally the customer's responsibility, but CSPs may provide support to incident response teams.

3. **Patching and Updating**

   1. CSPs are responsible for ensuring that their cloud offerings are secure and rapidly patch software within their purview but usually do not patch software managed by the customer

Source: NSA

NIST Holding Slide

● Sample Content Slide

1. **Content Point 1**

    1. Content Subpoint 1.1

2. **Content Point 2**

    1. Content Subpoint 2.1

Q&A