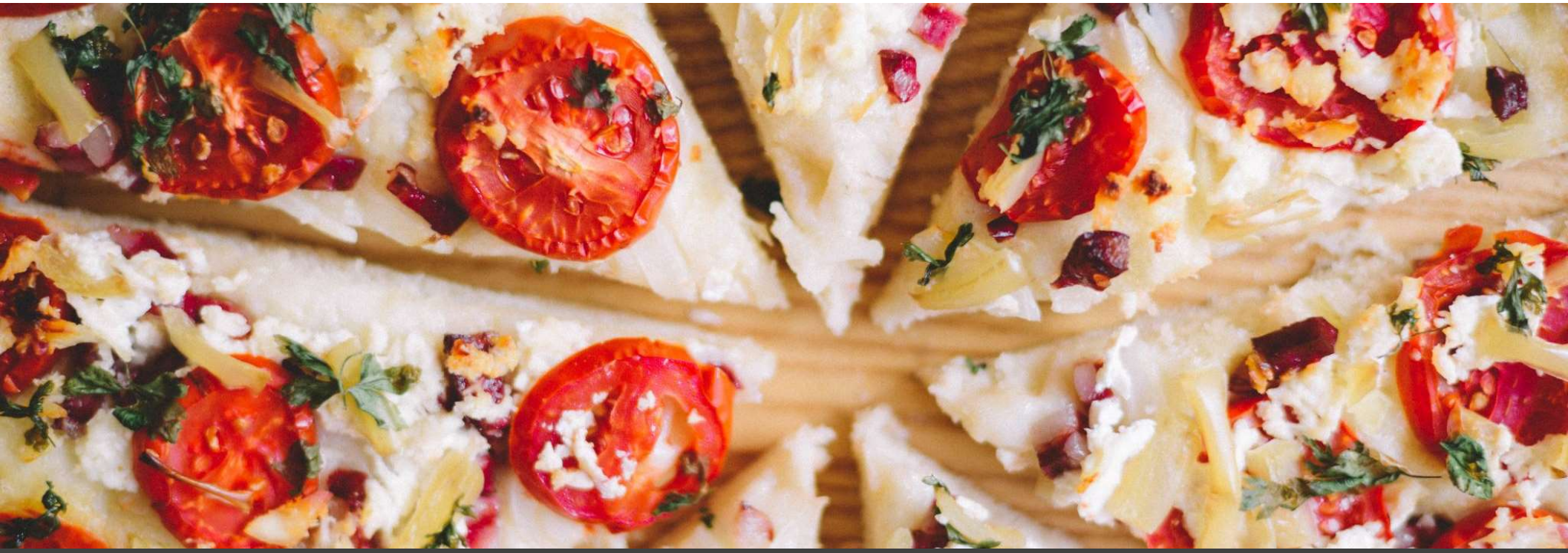


Validate the Security of the Cloud

Who am I?

- Security Evangelist
- ISACA emerging trends working group & VP at ISACA GWDC
- 25 years in cyber including 10 years as a CISO
- VP, security services at NTT DATA, top 10 global IT services focused on digital transformation
- CISSP,CCAK,CCSK,CRISC,CISA,CISM, CDPSE

You are having a Party!

Make it yourself

Go to a Restaurant

I have great cooking skills
I know I will use the best ingredients

I am a terrible cook

Make the food yourself

Go to a Restaurant

Why do you use third party services?

- We don’t have the right skills
- Not aligned with your “life objectives”
- We don’t have enough time
- We could save money or use our money in a different way, no reason to own a car, or a house
- Others??

Why would you choose one restaurant over another?

Choosing providers

- Reputation
- Personal experience
- Reliability
- Price
- No food safety violations
- More for less
- They have special ovens and equipment; we are unable to reproduce this

Decreasing the workload in IT

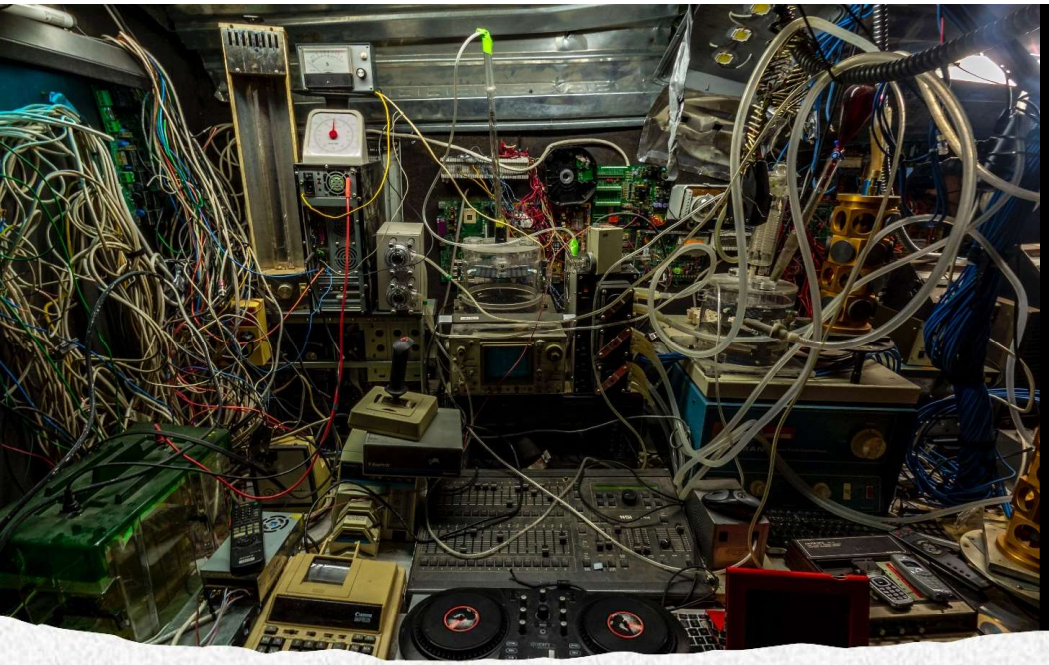
- That is what we did with cloud!
- We outsourced some of our IT to a third party
- Is that better than doing it ourselves?

Pizza as a Service 2.0

Tradition On-Premise (legacy)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	
Conversation	Conversation	Conversation	Conversation	Configuration
Friends	Friends	Friends	Friends	Functions
Beer	Beer	Beer	Beer	Scaling
Pizza	Pizza	Pizza	Pizza	Runtime
Fire	Fire	Fire	Fire	OS
Oven	Oven	Oven	Oven	Visualization
Electric/Gas	Electric/Gas	Electric/Gas	Electric/Gas	Hardware
Homemade	Communal Kitchen	Takeaway	Restaurant	

You Manage

Your Vendor Manages



Your server room?

The CSPs data center?

Your Kitchen

The Restaurant’s Kitchen

Cloud Service Delivery Models

SOFTWARE AS A SERVICE (SAAS)

PLATFORM AS A SERVICE (PAAS)

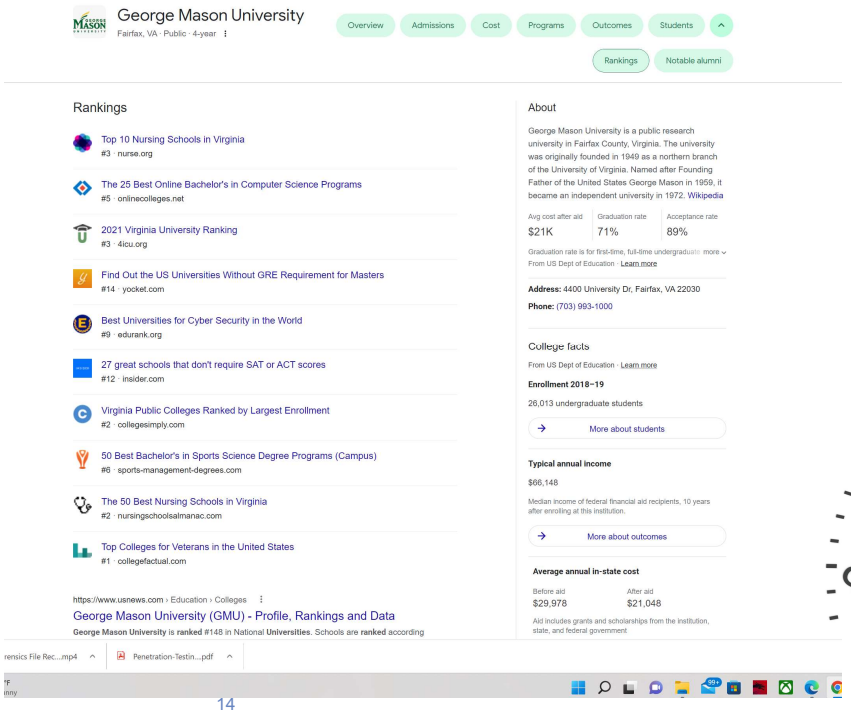
INFRASTRUCTURE AS A SERVICE (IAAS)

Its about Trust

What makes us trust someone to do what we have hired them to do and how do we do this in a systematic fashion?

Great Service

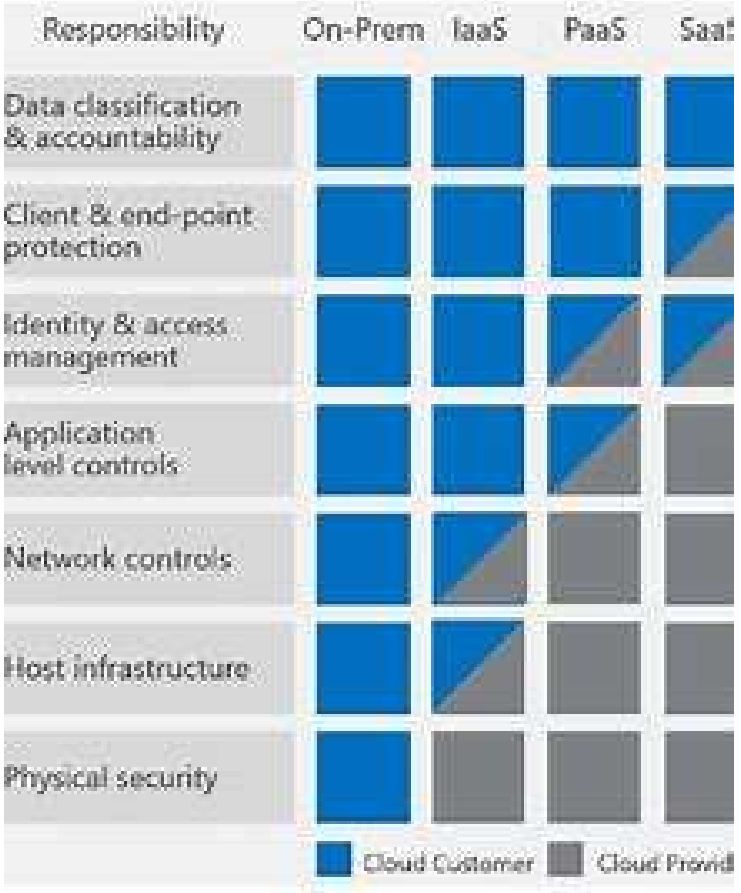
Excellent Five Stars



Cloud Shared Responsibility

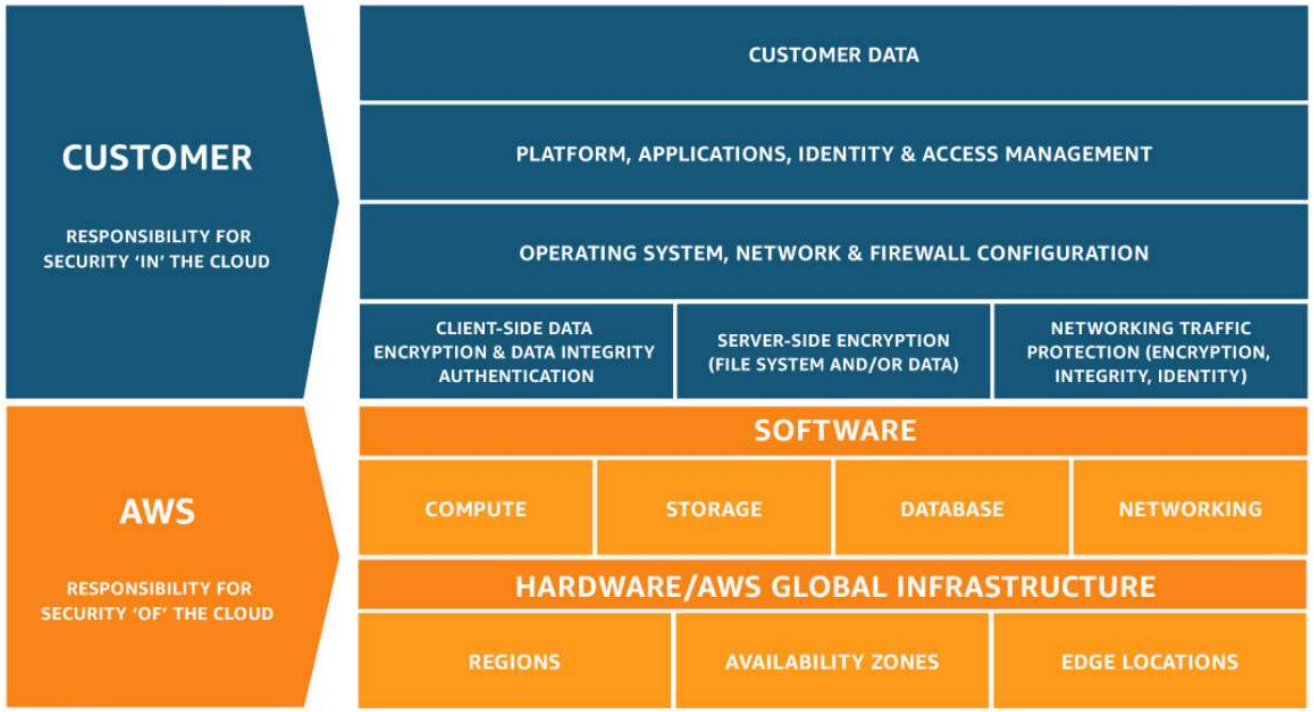
Security and Compliance is a shared responsibility between the CSP and the customer.

The responsibility changes according to the deployment model



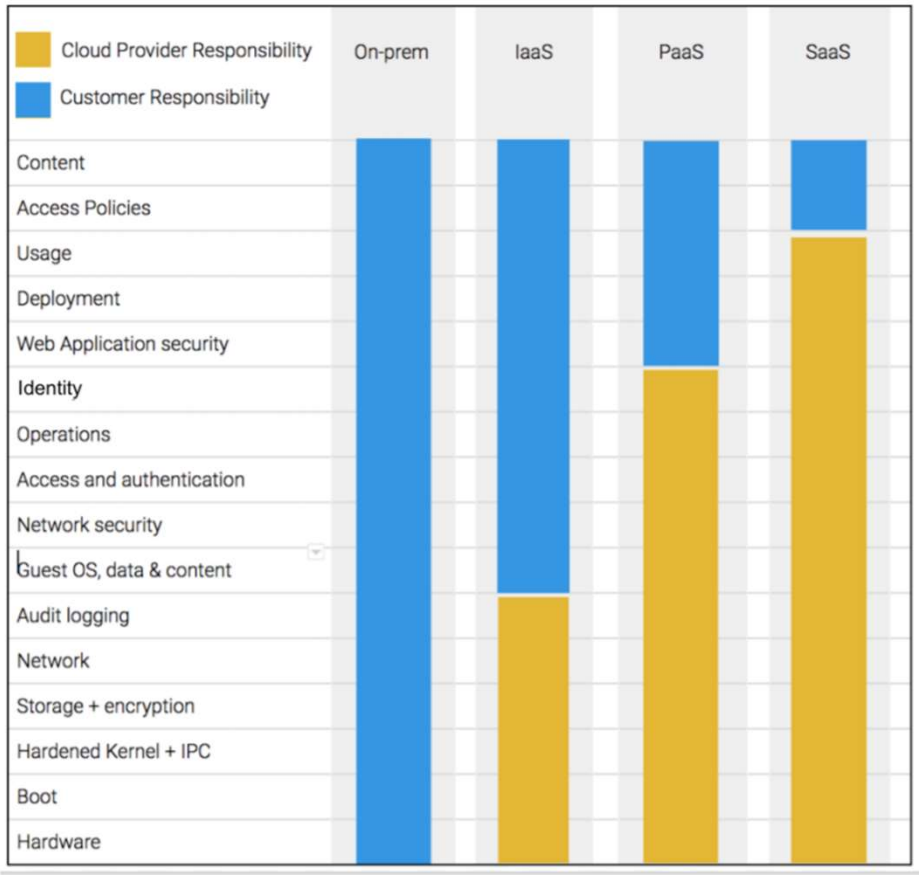
[Diagram from Shared Responsibility for Security Privacy and Compliance in Microsoft Azure]

AWS Shared responsibility Model



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

GCP Shared Responsibility Model



https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

Poll question

Which service model poses the most risk to the cloud consumer?

IaaS

SaaS

PaaS

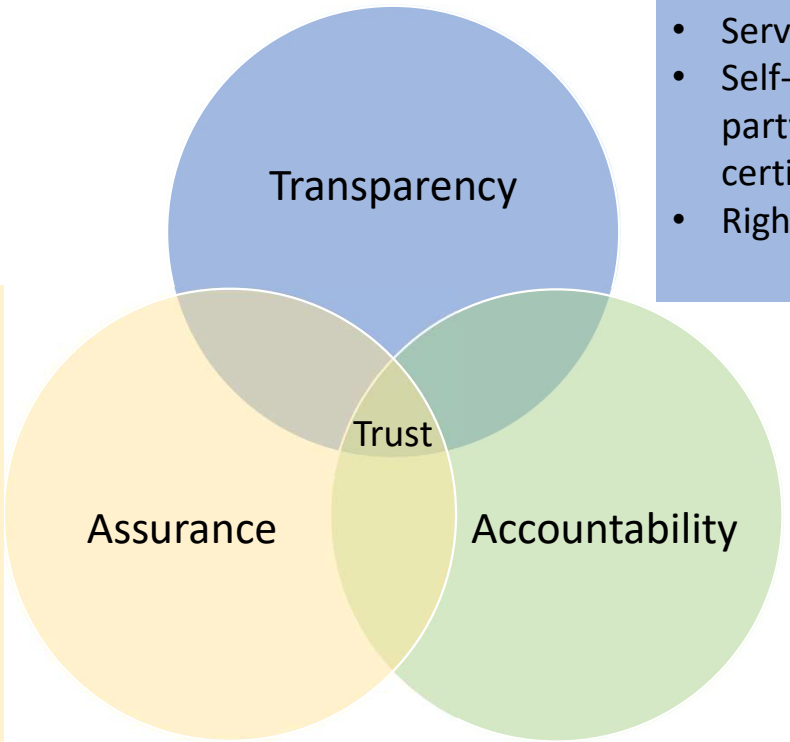
When does a team win?

- Everyone has a **role** in the team
- We all need to **agree** on who is responsible for what
- This is a supply chain issue
- One member playing badly could make the other team win

The foundations of cloud governance

When developing cloud governance programs, organizations must rely on four foundational pillars: trust, assurance, transparency and accountability.

- Security policies
- Service level agreement
- Self-assessment, third-party assessment and certification
- Right to Audit



- Contracts and terms of use, including service level agreements
- External attestation and certification audit reports (e.g., SOC2, ISO27001)
- Provider reputation
- Provider financial stability and market value
- Provider cyberinsurance

Responsiveness
Responsibility
Remediability

CLOUD COMPUTING Benefits

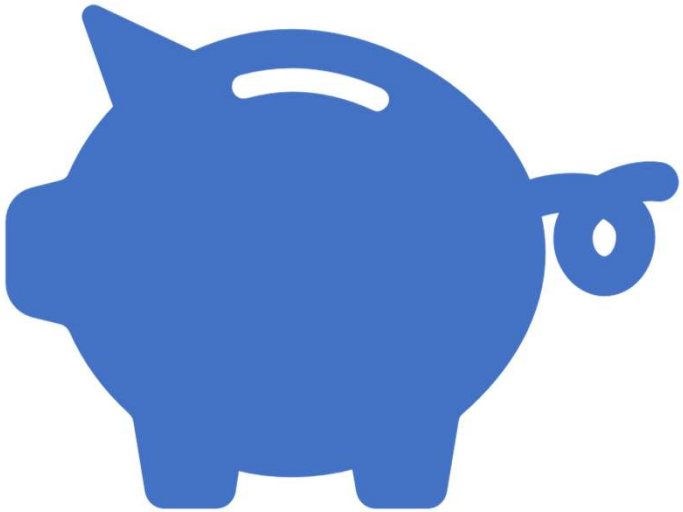
Cloud Computing refers to the use of resources available on the internet that have 5 essential characteristics; on demand self service, Broad network access, resource pooling, elasticity, measured service

What are the benefits of Cloud?

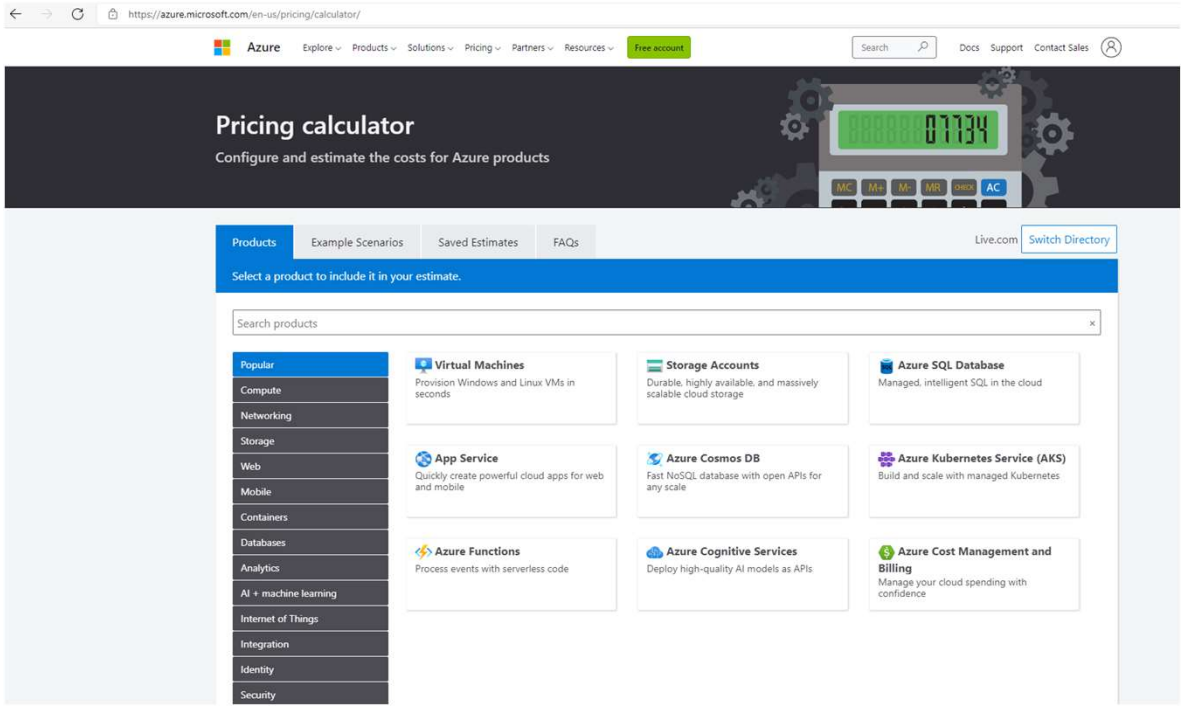
- Cost Saving
- Availability/Reliability
- Flexibility/Elasticity/Scalability
- Security
- Agility
- Optimized Resource Utilization
- Access to skills and capabilities
- Performance

Cloud definition from NIST SP 800-145, The NIST Definition of Cloud Computing

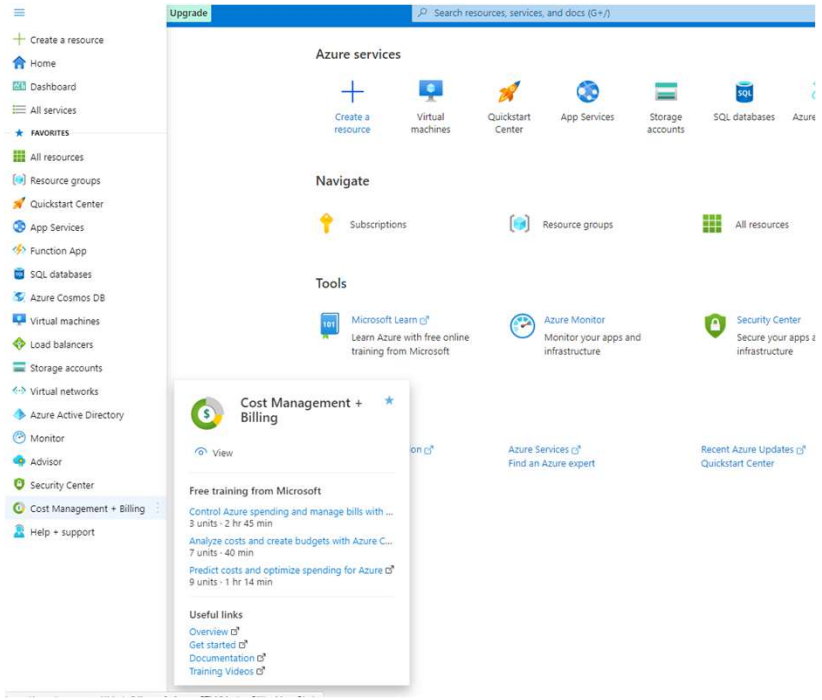
Cost Savings

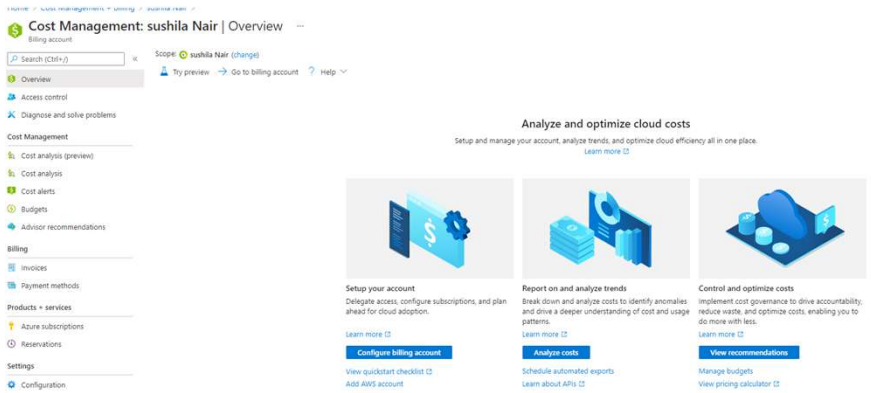


Projecting Cost (Before you Migrate)

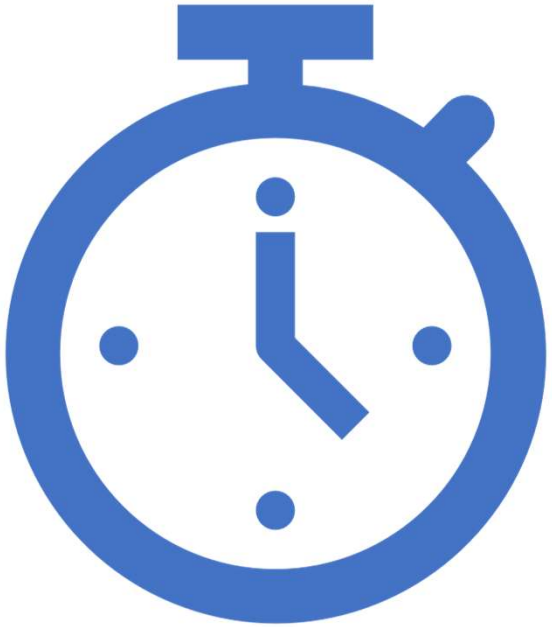


Understanding Cost after you migrate





Availability



Understanding Azure Zones and Regions

Azure Availability Zones are physically and logically separated datacenters with their own independent power source, network, and cooling. Connected with an extremely low-latency network, they become a building block to delivering high availability applications

A region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

To ensure resiliency, there's a minimum of three separate zones in all enabled regions

https://infrastructuremap.microsoft.com/

AWS Availability Zones

- An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region.
- All AZs in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between AZs. All traffic between AZs is encrypted.
- Each AWS Region has multiple AZs

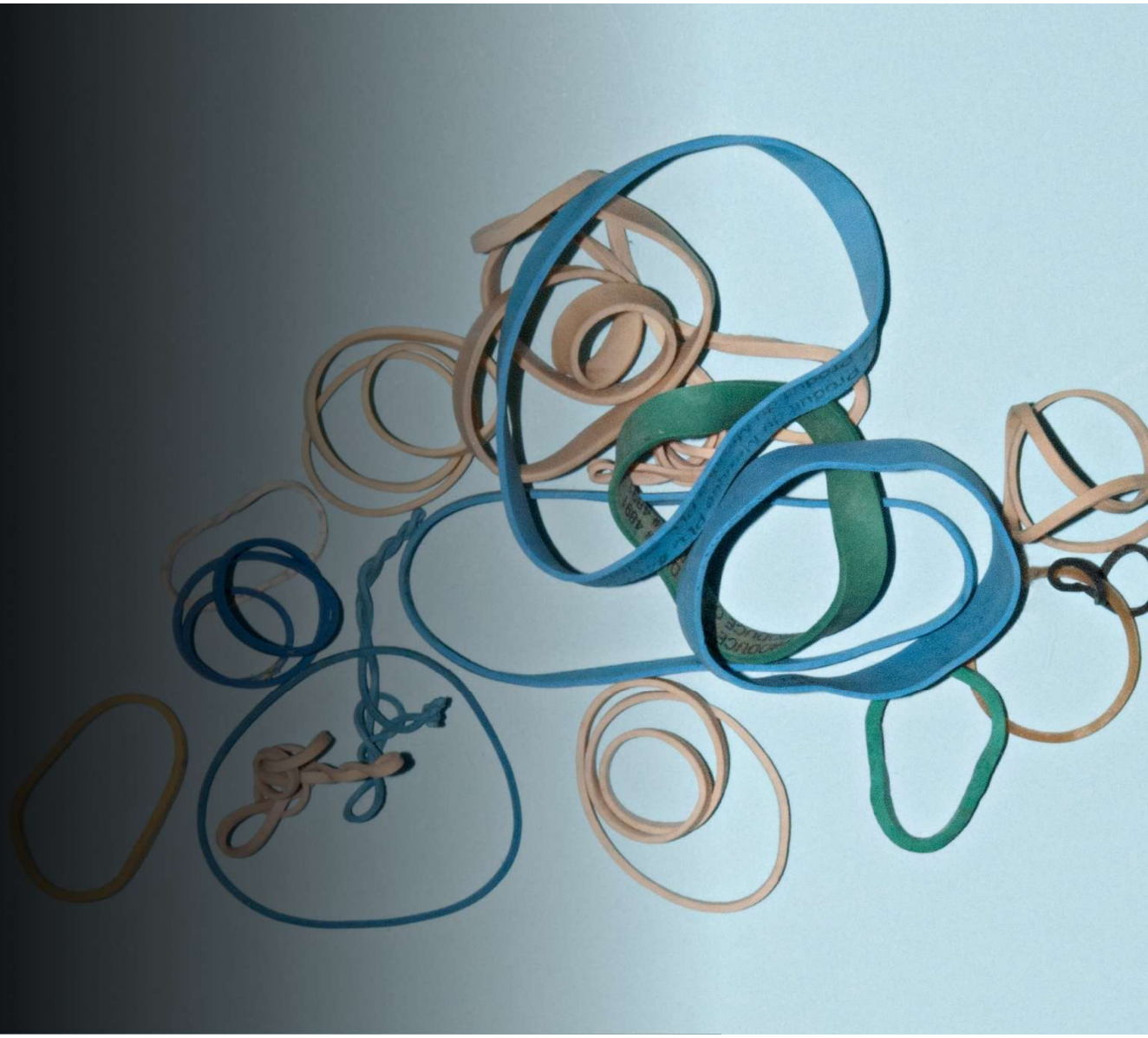
Image copyright Amazon

GCP Regions and Zones

- GCP locations are composed of regions and zones.
- A region is a specific geographical location where you can host your resources.
- Regions have three or more zones. For example, the us-west1 region denotes a region on the west coast of the United States that has three zones: us-west1-a, us-west1-b, and us-west1-c.

Image copyright Google

Elasticity



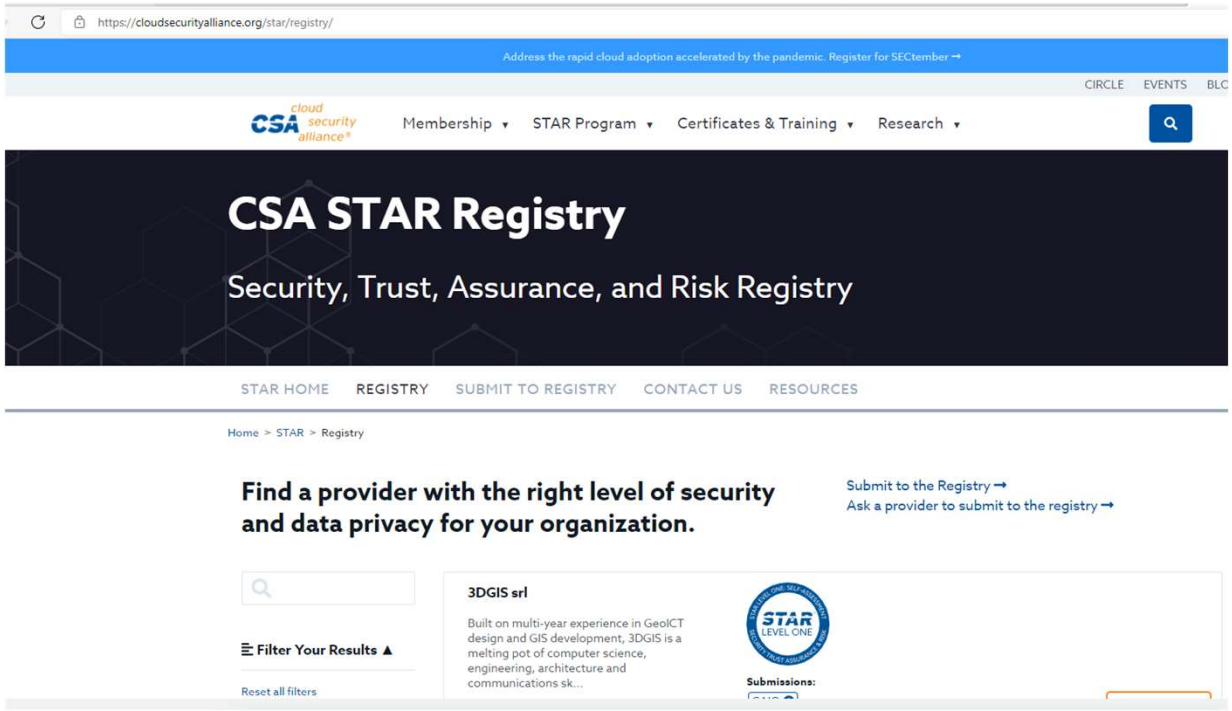
Scale sets

- Virtual machine scale sets let you create and manage a group of load balanced VMs.
- The number of VM instances can automatically increase or decrease in response to demand or a defined schedule.
- Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs.
- We recommended that two or more VMs are created within a scale set to provide for a highly available application There is no cost for the scale set itself, you only pay for each VM instance that you create.

GCP and AWS

- In GCP, Autoscaling is a feature of managed instance groups (MIGs). A managed instance group is a collection of virtual machine (VM) instances that are created from a common instance template. An autoscaler adds or deletes instances from a managed instance group based on the group's autoscaling policy.
- An *Auto Scaling group* contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

Defining Trust



- The CSA defines trust as a function of assurance, transparency and accountability
- The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings

Demo: CSA STAR

1. https://cloudsecurityalliance.org/star/registry/

Learning more about cybersecurity and Cloud

- Cybersecurity Fundamentals
- Security+
- CISSP
- CET
- CCSK
- CCAK (I am a authorized instructor)
- CCSP
- Cloud platform specific certs

Thank you

- Any questions???
- Contact nairsushi@gmail.com
- Follow me on LinkedIn https://www.linkedin.com/in/sushilanair/
- Twitter @sushila_nair

Community builds our skills and network