



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

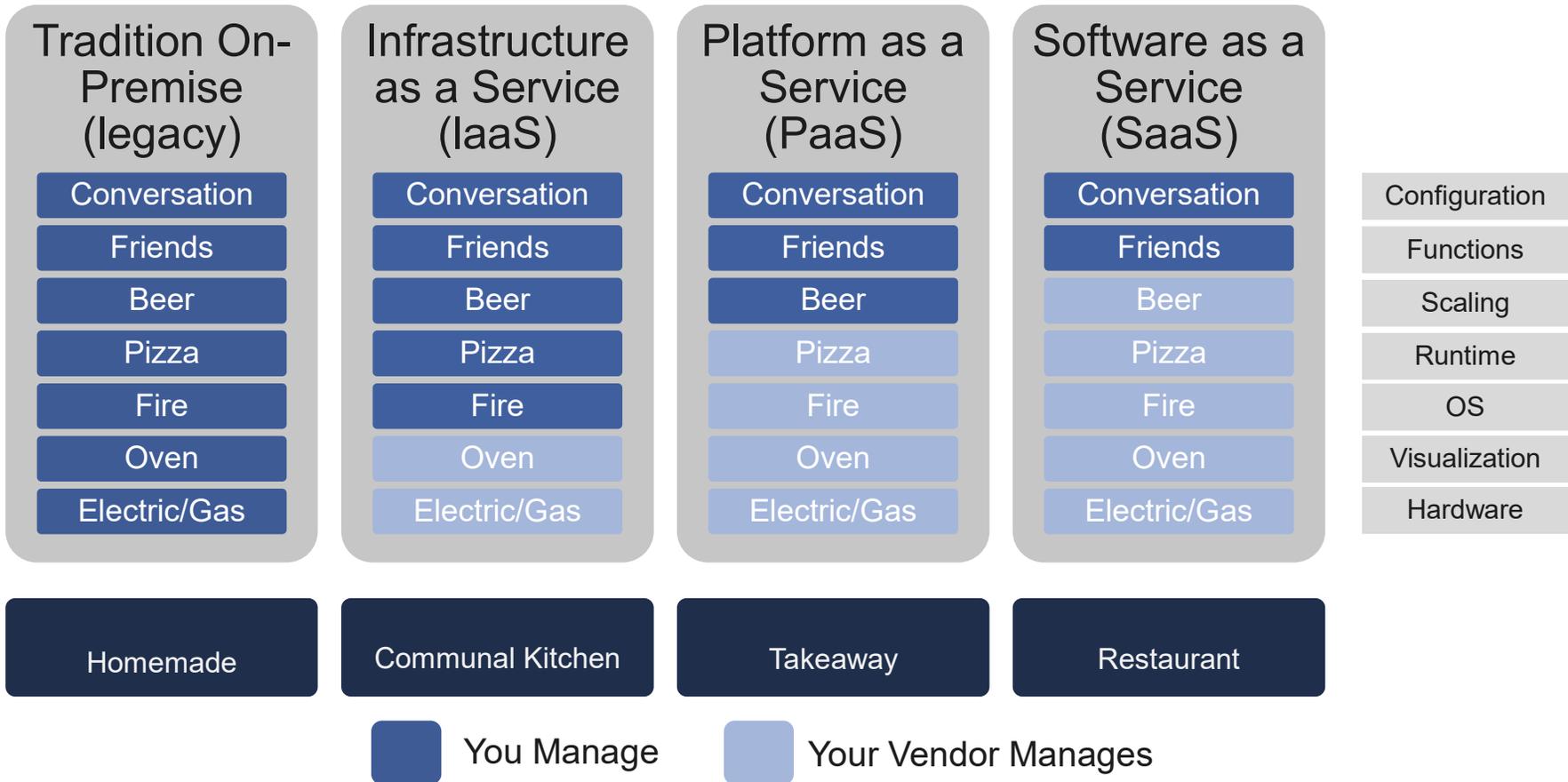
Decreasing the workload in IT

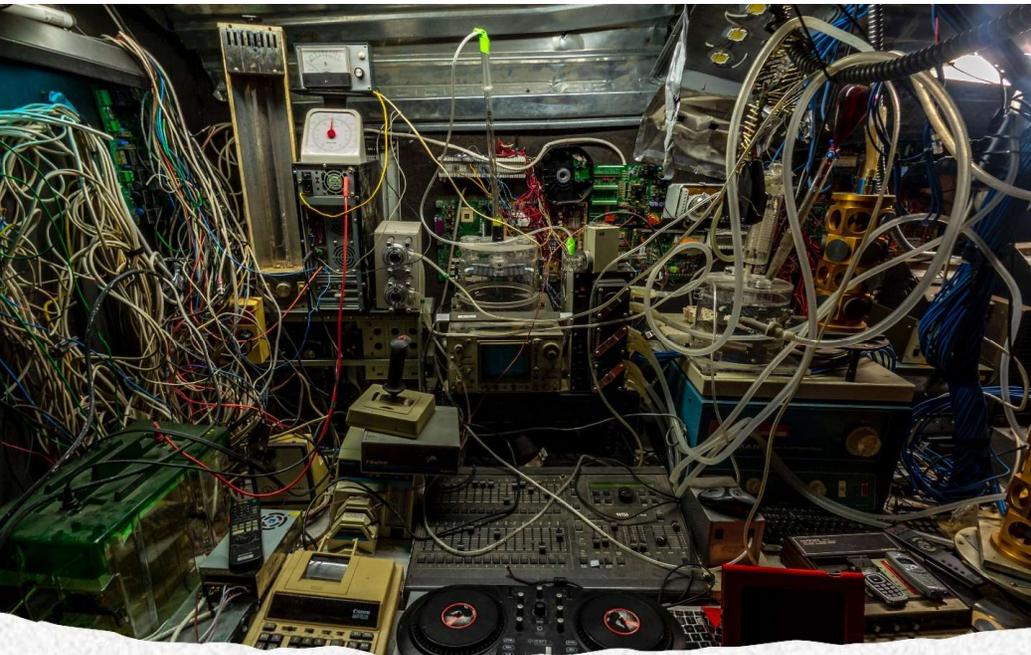
- That is what we did with cloud!
 - We outsourced some of our IT to a third party
 - Is that better than doing it ourselves?
-





Pizza as a Service 2.0





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

George Mason University
Fairfax, VA · Public · 4-year

Overview Admissions Cost Programs Outcomes Students

Rankings Notable alumni

Rankings

- Top 10 Nursing Schools in Virginia #3 - nurse.org
- The 25 Best Online Bachelor's in Computer Science Programs #5 - onlinecolleges.net
- 2021 Virginia University Ranking #3 - 4icu.org
- Find Out the US Universities Without GRE Requirement for Masters #14 - yocket.com
- Best Universities for Cyber Security in the World #9 - edurank.org
- 27 great schools that don't require SAT or ACT scores #12 - insalder.com
- Virginia Public Colleges Ranked by Largest Enrollment #2 - collegesimply.com
- 50 Best Bachelor's in Sports Science Degree Programs (Campus) #6 - sports-management-degrees.com
- The 50 Best Nursing Schools in Virginia #2 - nursing-schools-atmaniac.com
- Top Colleges for Veterans in the United States #1 - collegesfactual.com

https://www.usnews.com › Education › Colleges
George Mason University (GMU) - Profile, Rankings and Data
George Mason University is ranked #148 in National Universities. Schools are ranked according

About

George Mason University is a public research university in Fairfax County, Virginia. The university was originally founded in 1949 as a northern branch of the University of Virginia. Named after Founding Father of the United States George Mason in 1959, it became an independent university in 1972. Wikipedia

Avg cost after aid	Graduation rate	Acceptance rate
\$21K	71%	89%

Graduation rate is for first-time, full-time undergraduates. From US Dept of Education. [Learn more](#)

Address: 4400 University Dr, Fairfax, VA 22030
Phone: (703) 993-1000

College facts

From US Dept of Education. [Learn more](#)

Enrollment 2018-19
26,013 undergraduate students
[More about students](#)

Typical annual income

\$66,148

Median income of federal financial aid recipients, 10 years after enrolling at this institution.
[More about outcomes](#)

Average annual in-state cost

Before aid	After aid
\$29,978	\$21,048

Aid includes grants and scholarships from the institution, state, and federal government



Cloud Shared Responsibility

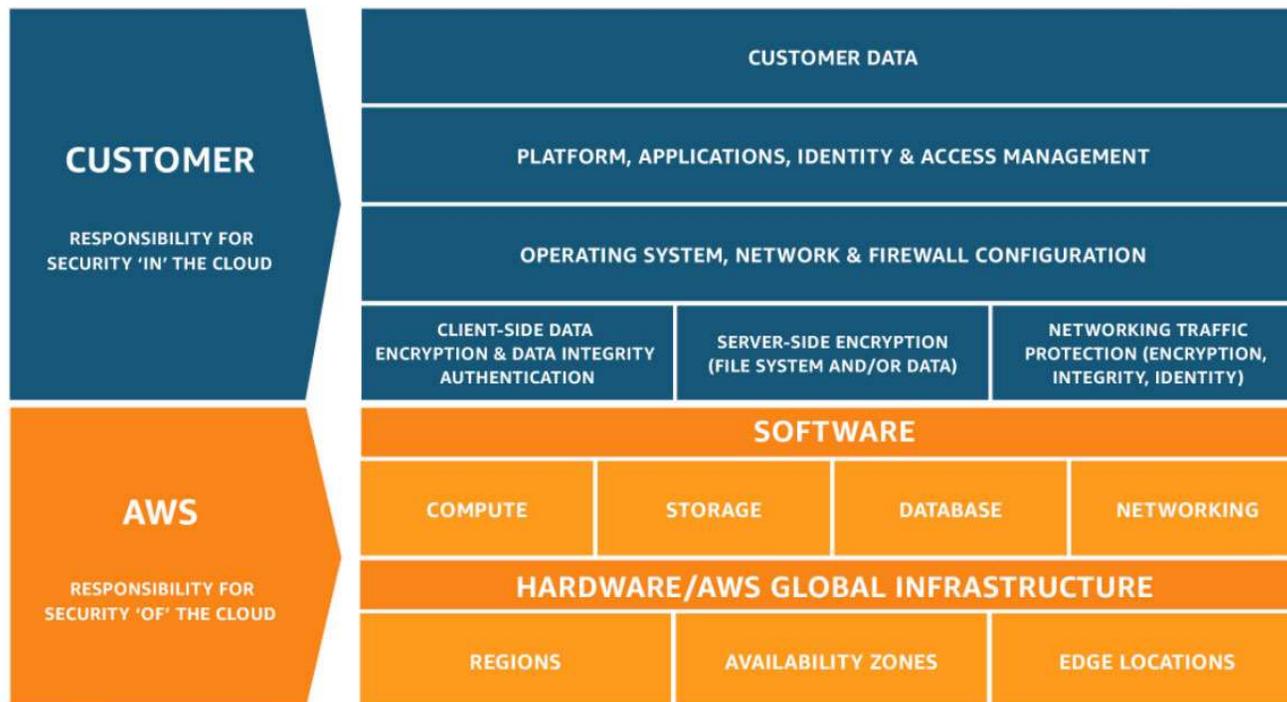
Security and Compliance is a shared responsibility between the CSP and the customer.

The responsibility changes according to the deployment model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Shared
Identity & access management	Cloud Customer	Cloud Customer	Shared	Shared
Application level controls	Cloud Customer	Cloud Customer	Shared	Cloud Provider
Network controls	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: Cloud Customer (Blue), Cloud Provider (Grey)

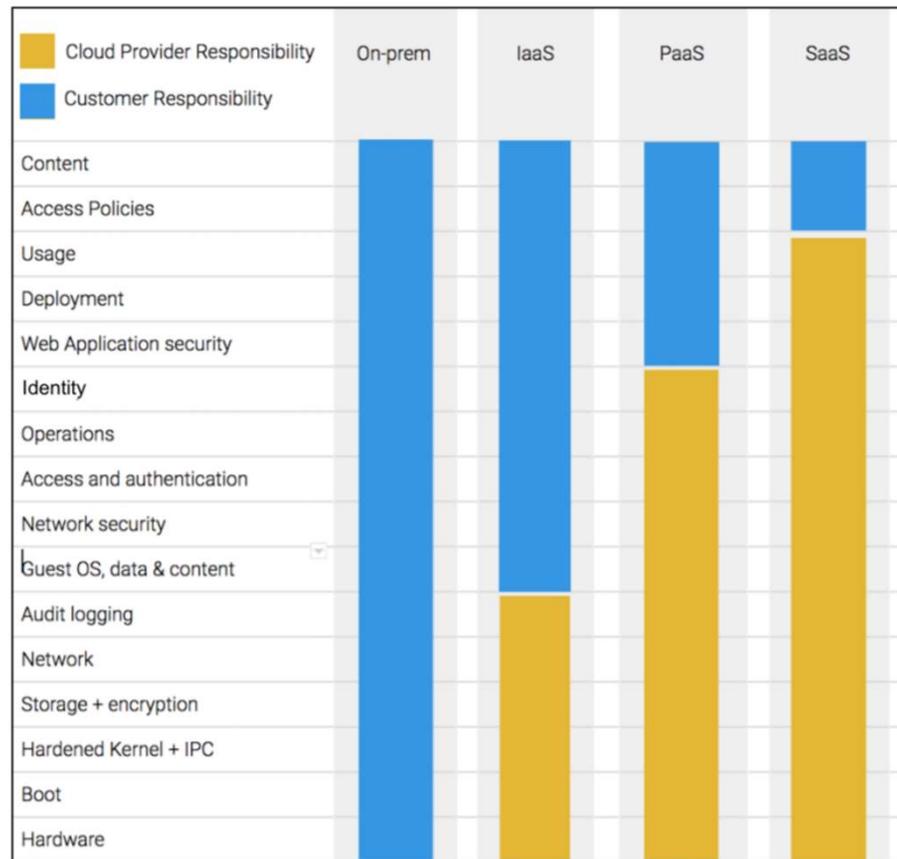
AWS Shared responsibility Model



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

Copyright Amazon

GCP Shared Responsibility Model



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

Copyright Google

Poll question

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

IaaS

SaaS

PaaS



When does a team win?

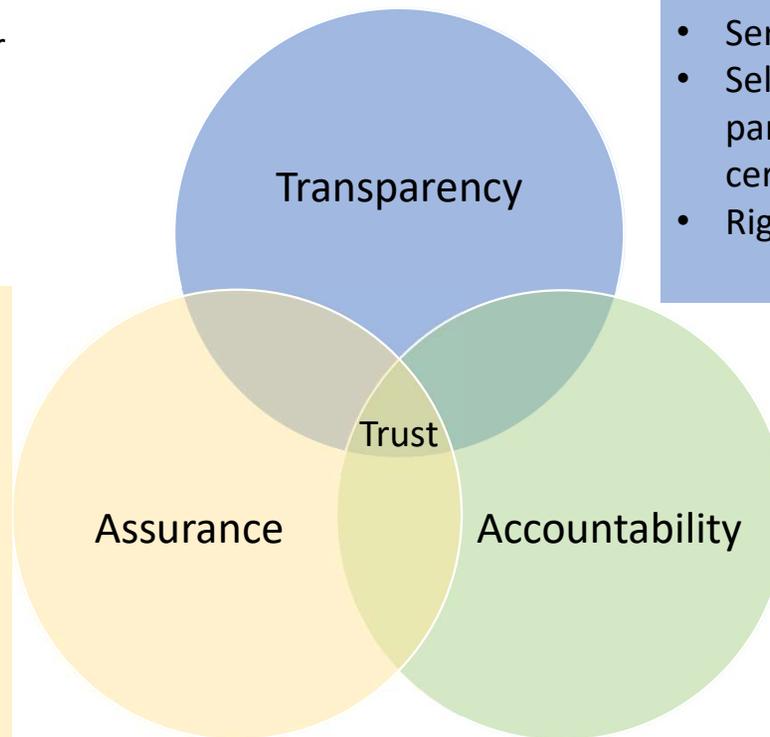
- Everyone has a **role** in the team
 - We all need to **agree** on who is responsible for what
 - This is a supply chain issue
 - One member playing badly could make the other team win
-



The foundations of cloud governance

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

- 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



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

Responsiveness
Responsibility
Remediability

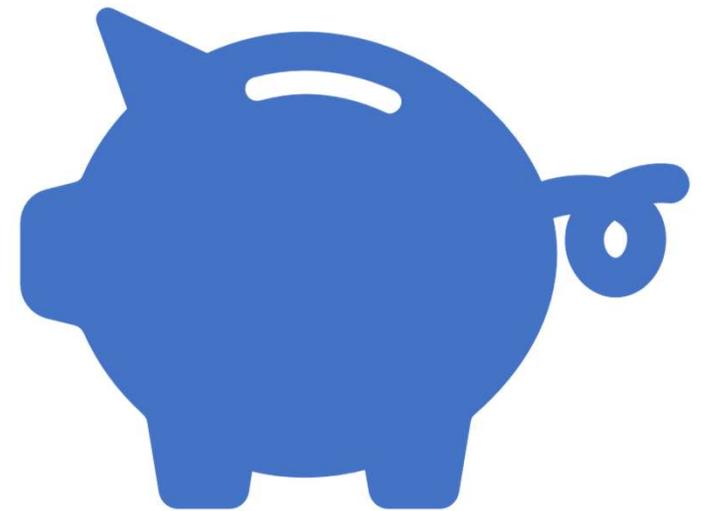
CLOUD COMPUTING Benefits

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

Cost Savings



Projecting Cost (Before you Migrate)

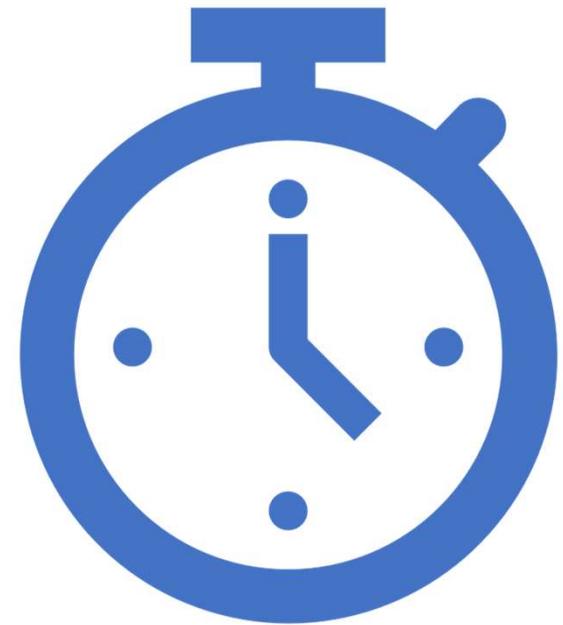
The screenshot shows the Azure Pricing Calculator interface. At the top, the URL is <https://azure.microsoft.com/en-us/pricing/calculator/>. The navigation bar includes links for Azure, Explore, Products, Solutions, Pricing, Partners, Resources, and a Free account button. A search bar and links for Docs, Support, and Contact Sales are also present. The main heading is "Pricing calculator" with the subtext "Configure and estimate the costs for Azure products". Below this, there are tabs for Products, Example Scenarios, Saved Estimates, and FAQs. A "Live.com" link and a "Switch Directory" button are on the right. A blue bar prompts the user to "Select a product to include it in your estimate." Below this is a search bar for products. A sidebar on the left lists various categories: Popular, Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, AI + machine learning, Internet of Things, Integration, Identity, and Security. The main content area displays several product cards: Virtual Machines (Provision Windows and Linux VMs in seconds), Storage Accounts (Durable, highly available, and massively scalable cloud storage), Azure SQL Database (Managed, intelligent SQL in the cloud), App Service (Quickly create powerful cloud apps for web and mobile), Azure Cosmos DB (Fast NoSQL database with open APIs for any scale), Azure Kubernetes Service (AKS) (Build and scale with managed Kubernetes), Azure Functions (Process events with serverless code), Azure Cognitive Services (Deploy high-quality AI models as APIs), and Azure Cost Management and Billing (Manage your cloud spending with confidence). A digital display in the top right corner shows the number 07734.

Understanding Cost after you migrate

The screenshot shows the Azure portal home page. The left sidebar contains navigation options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main area is titled 'Upgrade' and features a search bar and several sections: 'Azure services' (Create a resource, Virtual machines, Quickstart Center, App Services, Storage accounts, SQL databases, Azure), 'Navigate' (Subscriptions, Resource groups, All resources), and 'Tools' (Microsoft Learn, Azure Monitor, Security Center). A 'Cost Management + Billing' tile is highlighted, showing 'Free training from Microsoft' with three links: 'Control Azure spending and manage bills with ... 3 units - 2 hr 45 min', 'Analyze costs and create budgets with Azure C... 7 units - 40 min', and 'Predict costs and optimize spending for Azure 9 units - 1 hr 14 min'. Below this are 'Useful links' for Overview, Get started, Documentation, and Training Videos.

The screenshot shows the 'Cost Management: sushila Nair | Overview' page. It includes a search bar, a 'Scope' dropdown set to 'sushila Nair (change)', and a 'Try preview' button. A table of contents lists sections: Overview, Access control, Diagnose and solve problems, Cost Management (Cost analysis, Cost analysis (preview), Cost alerts, Budgets, Advisor recommendations), Billing (Invoices, Payment methods), Products + services (Azure subscriptions, Reservations), Settings (Configuration), Support + troubleshooting, and New support request. The main content area is titled 'Analyze and optimize cloud costs' and includes three cards: 'Setup your account', 'Report on and analyze trends', and 'Control and optimize costs'. Each card has a 'Learn more' link and a 'View recommendations' button.

Availability



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

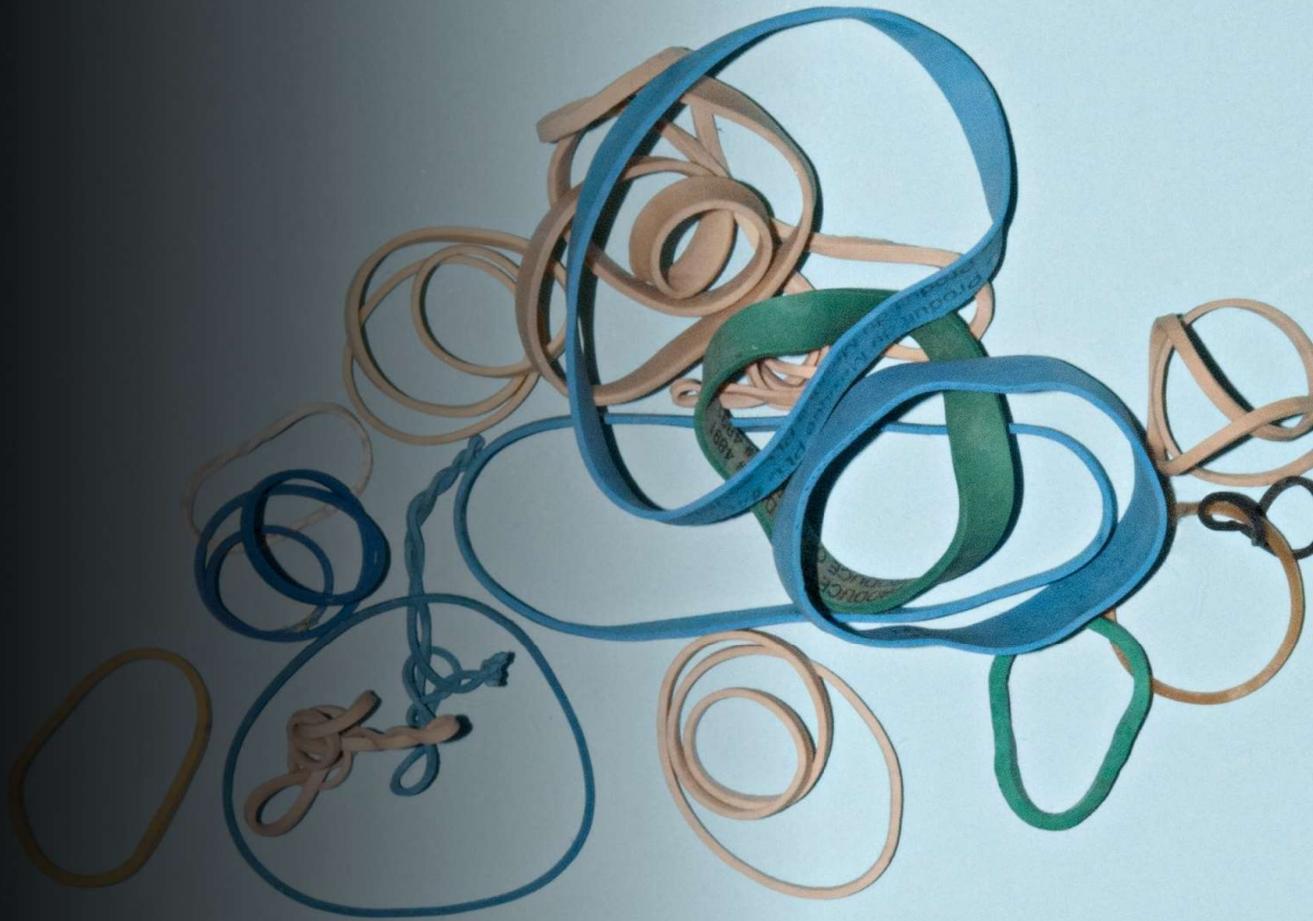
GCP Regions and Zones



- 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.



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

Address the rapid cloud adoption accelerated by the pandemic. Register for SECTember →

CIRCLE EVENTS BLC

cloud security alliance® Membership ▾ STAR Program ▾ Certificates & Training ▾ Research ▾

CSA STAR Registry

Security, Trust, Assurance, and Risk Registry

STAR HOME REGISTRY SUBMIT TO REGISTRY CONTACT US RESOURCES

Home > STAR > Registry

Find a provider with the right level of security and data privacy for your organization.

Submit to the Registry →
Ask a provider to submit to the registry →

Filter Your Results ▲

Reset all filters

3DGIS srl

Built on multi-year experience in GeolCT design and GIS development, 3DGIS is a melting pot of computer science, engineering, architecture and communications sk...

STAR LEVEL ONE

Submissions: []

- 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

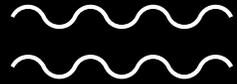
1. <https://cloudsecurityalliance.org/star/registry/>



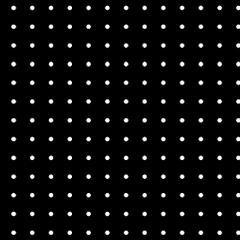
Learning more about cybersecurity and Cloud

- 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](https://twitter.com/sushila_nair)

Community builds our skills and network