



Risk Revolution

Cybersecurity and Auditing in the
Age of Disruption

Who am I?

- Security Evangelist
- ISACA emerging trends working group & VP at ISACA GWDC
- 25 years in cyber including 10 years as a CISO
- CISSP, CCAK, CCSK, CRISC, CISA, CISM, CDPSE, GIAC



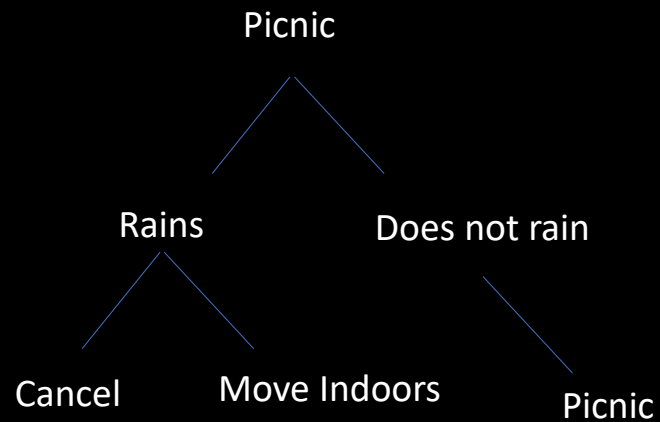
Agenda

- Introduction to Risk Management
- Understanding threats, risks and Zero Trust
- How Cloud Changes Everything

Risk management is the backbone
of the IT auditing process



Event Tree: Planning a Picnic



- **Starting Point:** The day of the picnic.
 - **First Branch:** It either rains or it doesn't.
 - **If it rains:** You can either move the picnic indoors or cancel it.
 - **If it doesn't rain:** The picnic goes ahead as planned outdoors.
 - **Further Branches:** If moved indoors, you can have either a fun gathering with games or a simple meal.
- This tree helps you see all possible outcomes and make plans for each scenario.

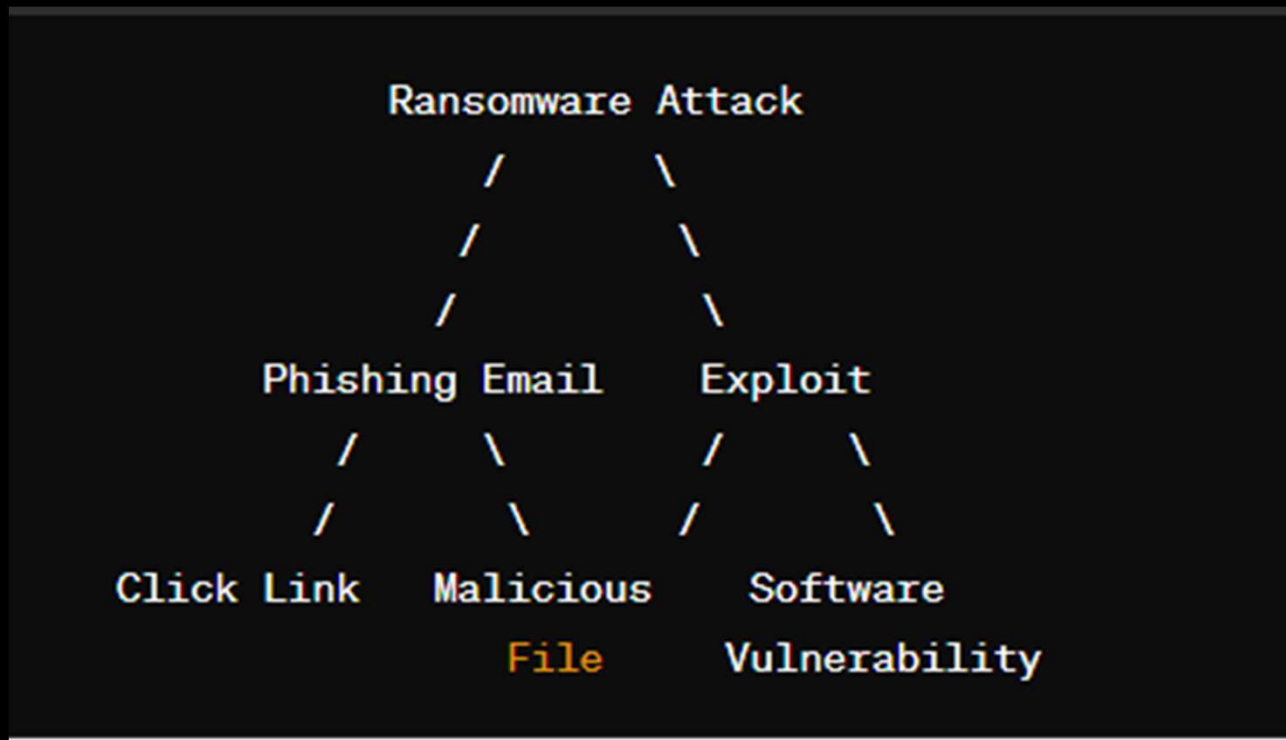
Event Tree Exercise

Try this with a Ransomware attack

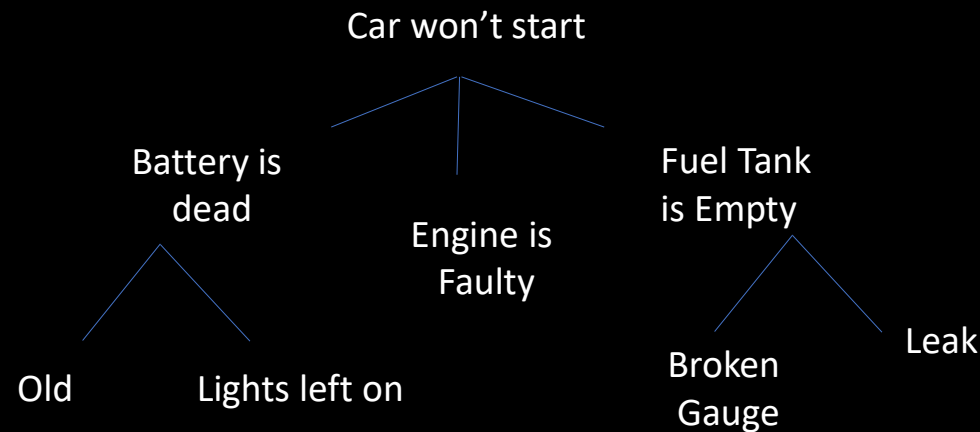
– Choose 2 events that could have caused it and build it from there

Why is this valuable?

Event Tree



Fault Tree: Car Won't Start



Fault tree analysis is used to trace the root causes of a failure.

Suppose your car won't start. The tree starts with the top event (car won't start) and works down to possible causes.

Top Event: Car won't start.

Major Causes: Battery is dead, fuel tank is empty, or engine is faulty.

Battery is Dead: Either the battery is old, or the lights were left on.

Fuel Tank is Empty: Either the gauge is broken, and you didn't realize, or it has a leak.

Engine is Faulty: Could be due to lack of maintenance or a failed component.

This analysis helps in identifying potential points of failure and mitigating them.

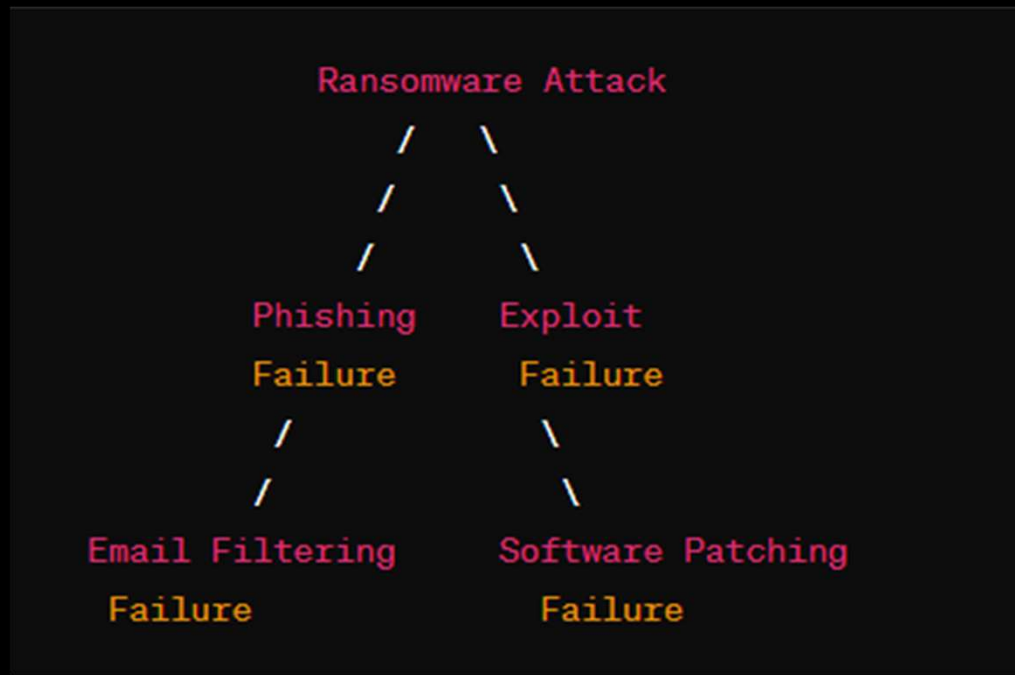
Exercise

Try this with a Ransomware attack

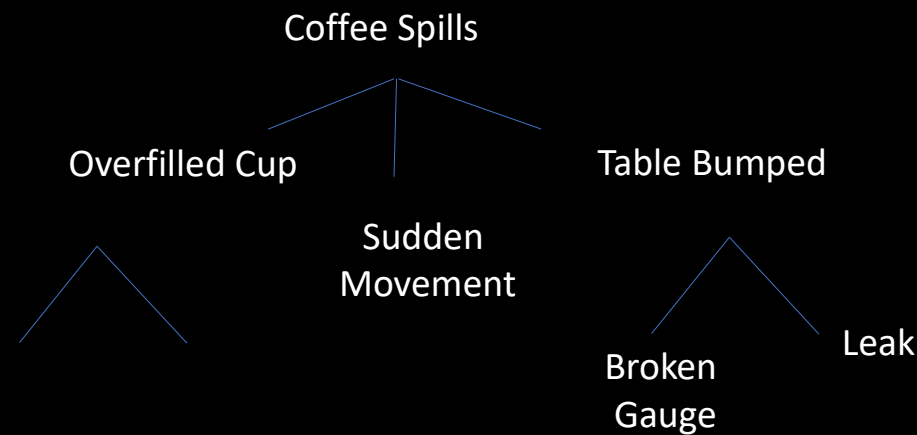
– Choose 2 events that could have caused it and build it from there

Why is this valuable?

Fault tree



Cause-Consequence Analysis: Spilling Coffee



This method is used to explore the consequences of a specific initiating event along with its causes.

Initiating Event: Coffee spills during a meeting.

Immediate Causes: Overfilled cup, sudden movements, table bumped.

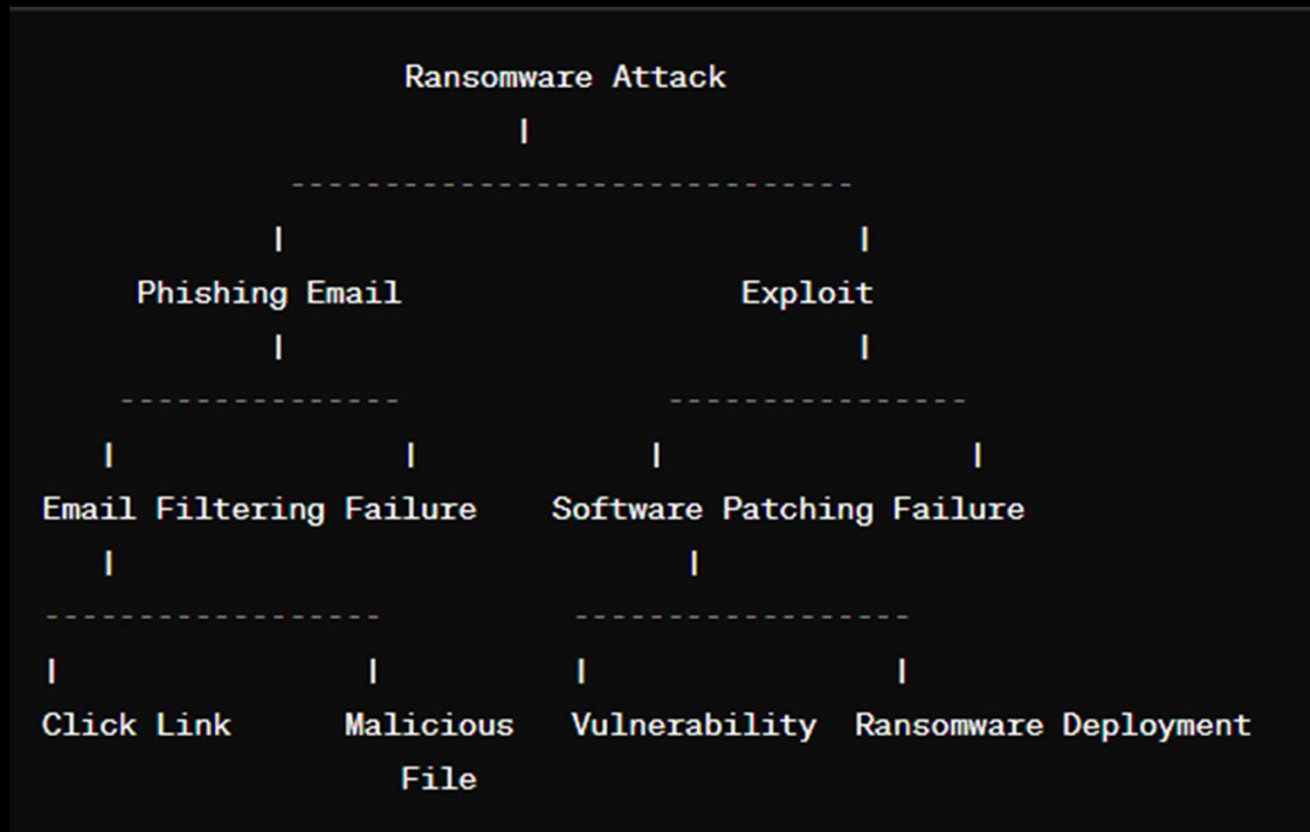
Consequences:

Short-term: Need to clean up, potential delay in meeting, minor burns.

Long-term: Could lead to more careful handling of beverages or a change in meeting protocol to avoid similar incidents.

In this analysis, you explore both the roots of the event and its impacts, allowing for comprehensive risk management strategies to be developed.

Cause Consequence analysis



Time Based Security

Protection > Detection + Response

Thinking about risk



Image from 99 Everyday Homes for Queenslanders (Brisbane: Home Building Publishing Co., 1939). Via Wikimedia Commons; public domain.

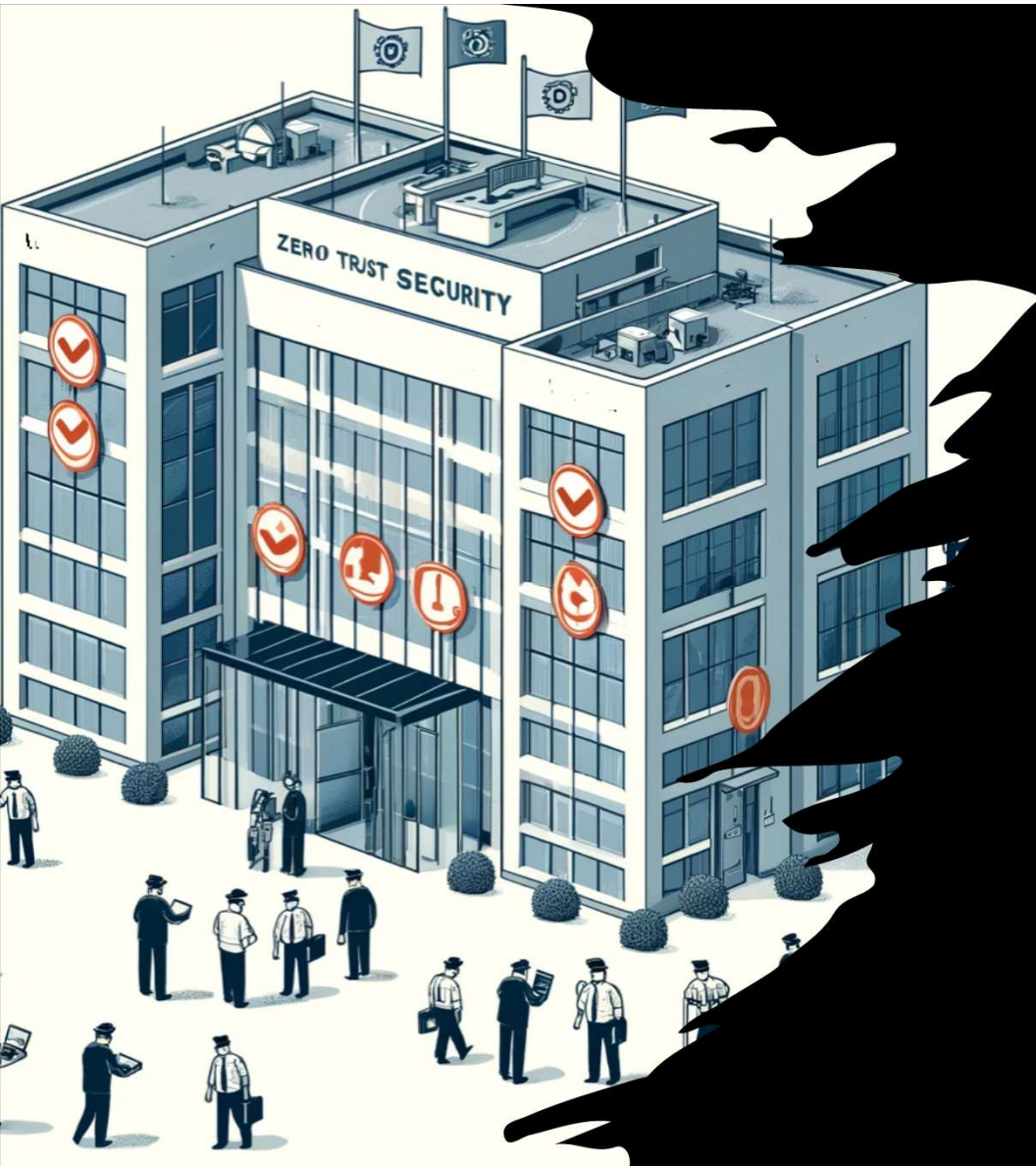
Key:

 Window (double)	 Indoor motion sensor \$50	 Indoor Camera \$500	 Window bars
 Door			
 Outdoor Camera \$1,000	Cloud based storage for video recording \$500 per year		

Provide labels here for any symbols you use!



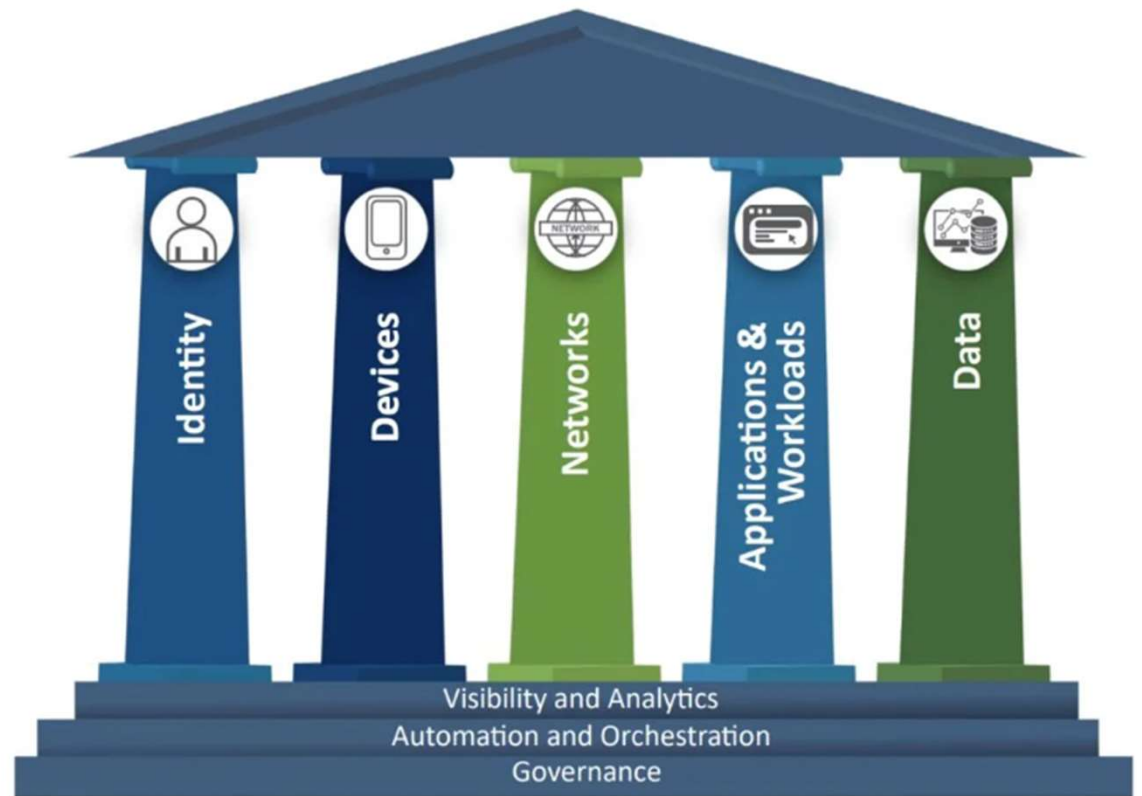
Zero Trust



Zero Trust is a cybersecurity philosophy based on the principle that organizations should not automatically trust anything inside or outside their perimeters and instead must verify everything trying to connect to their systems before granting access.

- **Never Trust, Always Verify:** Zero Trust is like having a bouncer at every door and window of your house, checking the ID of anyone who wants to come in, every single time, no matter if they live there or are just visiting.
- **Verify and then Trust:** Think of Zero Trust as the digital equivalent of double-checking that someone has the right key before letting them into a locked room, even if you've seen them use the key before.
- **Security Everywhere:** It's like putting a lock on every single door in a building, not just the front door. Everyone needs the right key and the right permissions to move from room to room.
- **Least Privilege Access:** This part of Zero Trust is like giving janitors keys that only open doors to the floors they need to clean, ensuring no one has more access than they need for their specific tasks.
- **Continuous Verification:** Imagine a security system that continuously checks if the people inside a building should still be there, not just at the moment they enter.

Zero Trust



Source: CISA

Moving From Implicit Trust to Zero Trust

Zero Trust

Request Context:

Identity

Unusual behavior?
Risky user's activity?
Unusual location?
Multi-factor Auth?

Device

Registered device?
Resource privileged?
Device compromised?

Application

Known application?
Is it sanctioned?
Password on web?

Network

Risk of the source?
Internal Request?
Configured to policy?
Is it privileged?

Infrastructure

What is the IP?
Compliant policy?
Managed proxy?

Data

Data location?
Data encrypted?
Data sensitivity?

Under a Zero Trust policy, greater context and comprehensive verification means more control and tighter security

Zero Trust Verification

Known Trusted
Allowed

Level of Assurance Required



Identity

How do I know who to trust and what to trust them with if we don't have a unified view of Identity?

IGA

Access Management

PAM

IDaaS

Saviynt
SailPoint

OKTA
EntraID

Cyberark
Delinea

OKTA



These components work together to make sure that the right people have the right access to the right information, just like in a well-organized school.



Device

Device Authentication and
Authorization

Device Security Posture Assessment

Device Health and Integrity

Secure Device Management

Least Privilege Access

Continuous Monitoring and Logging

Traditional Model



Zero Trust Model



Abandon the concepts of network-based connectivity and instead connect users to applications



Applications

- Application Authentication and Authorization
 - Secure Application Development
 - Application-Level Encryption
 - Application Monitoring and Anomaly Detection
 - Patch Management and Vulnerability Scanning
 - API Security
 - Logging and Auditing
- 

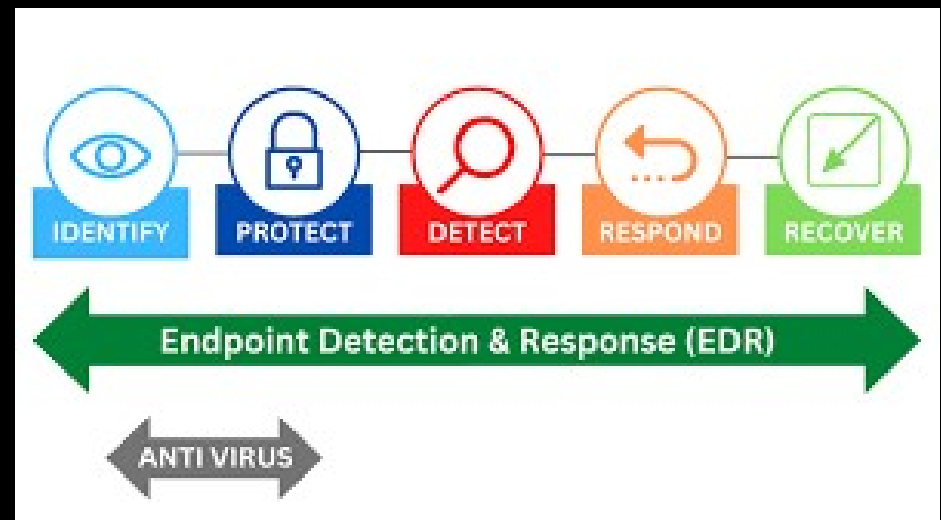


Encryption and Data Protection:

- Encrypt sensitive data both in transit and at rest to prevent unauthorized access and data exfiltration.
- Implement data loss prevention (DLP) solutions to monitor and enforce policies governing the use and transmission of sensitive information.
- Use secure protocols and encryption standards to secure communications between users, devices, and applications.

Continuous Monitoring and Analytics:

- Deploy network monitoring tools and security analytics platforms to detect and respond to anomalous behavior in real-time.
- Use behavioral analytics and machine learning algorithms to identify potential threats and deviations from normal patterns of user activity.
- Implement endpoint detection and response (EDR) solutions to monitor and remediate security incidents on endpoints.









How could
use Zero Trust
principles in
your
architecture?



Image from 99 Everyday Homes for Queenslanders (Brisbane: Home Building Publishing Co., 1939). Via Wikimedia Commons; public domain.

Key:

 Window (double)	 Indoor motion sensor \$50	 Indoor Camera \$500	 Window bars
 Door	 Outdoor Camera \$1,000	Cloud based storage for video recording \$500 per year	

Provide labels here for any symbols you use!



Threat modelling





- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Could you
use STRIDE
for our
house?



Image from 99 Everyday Homes for Queenslanders (Brisbane: Home Building Publishing Co., 1939). Via Wikimedia Commons; public domain.

Key:

	Window (double)		Indoor motion sensor \$50		Indoor Camera \$500		Window bars
	Door		Outdoor Camera \$1,000	Cloud based storage for video recording \$500 per year			

Provide labels here for any symbols you use!

Threat modelling

- **Spoofing:** We'll set up strong gates with guards who check everyone's IDs before they enter the house. This way, we make sure no sneaky impostors can pretend to be friendly visitors.
- **Tampering:** We'll build sturdy walls around the house and regularly check them for any cracks or holes. We'll also use security cameras to watch out for anyone trying to mess with our walls or decorations.
- **Repudiation:** We'll keep records of everyone who enters and leaves the house, like a guestbook. If someone causes trouble, we'll have proof of who did it, so they can't deny their actions later.
- **Information Disclosure:** We'll encrypt any messages or packages sent to and from the house, like putting secret codes on them. This way, even if someone tries to peek at our messages, they won't understand them.
- **Denial of Service:** We'll have backup entrances and exits to the house, so if one gets blocked, we can still get in and out. We'll also set up extra guards to keep an eye out for any troublemakers trying to block our paths.
- **Elevation of Privilege:** We'll have strict rules about who can do what in the house. Only trusted guards will have access to the keys and controls, so no one can sneak in and try to take over.



Why does cloud change
everything?



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
5 or less people
Equipment

Make the food yourself



I am a terrible cook
5 or more people
Pricing

Go to a Restaurant

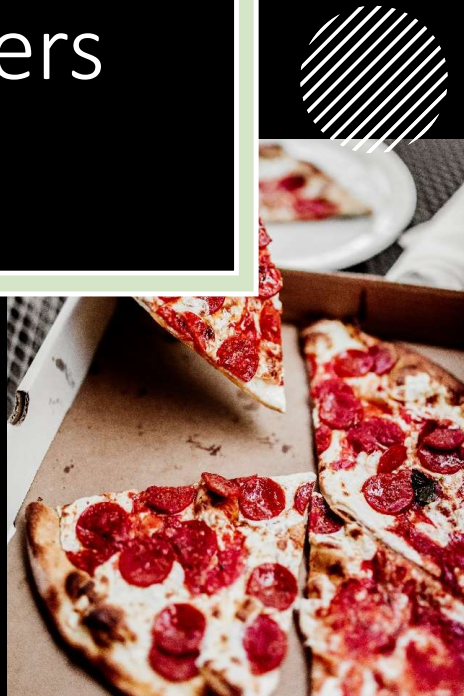
Why do you use third party services?

- 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

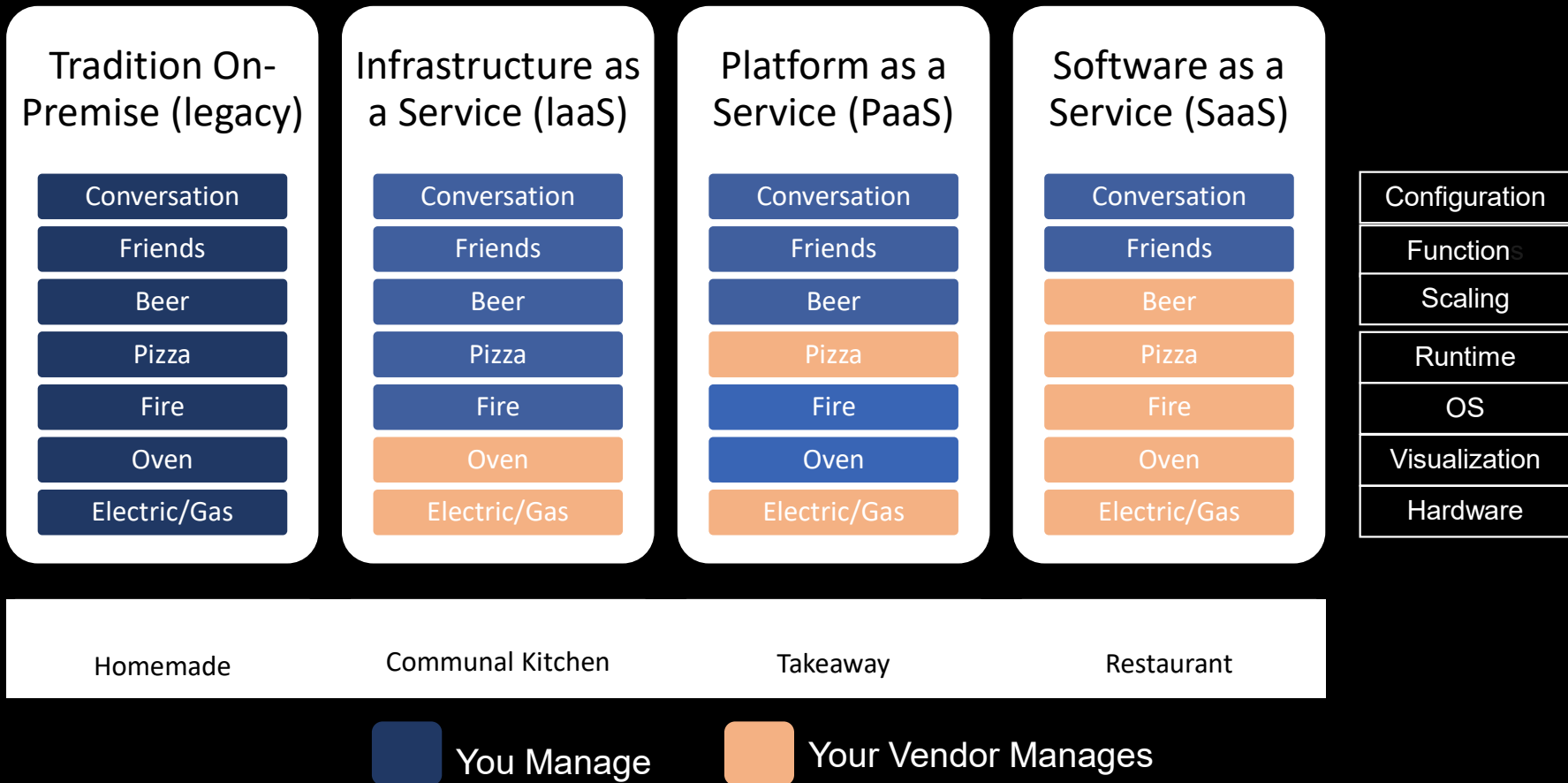
Decreasing the workload in IT

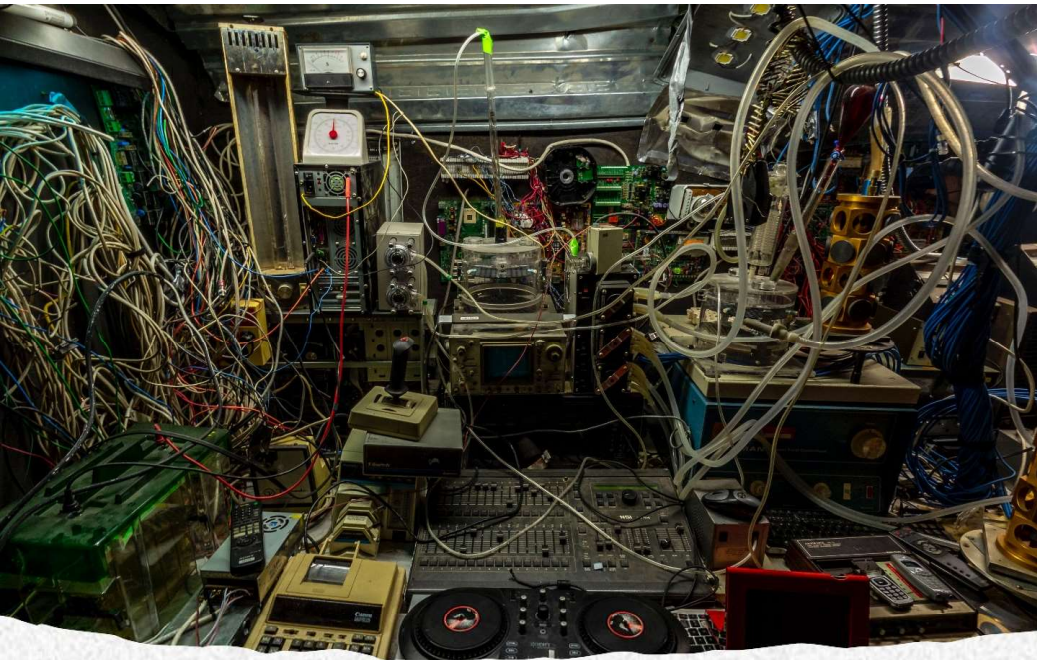
- That is what we did with cloud!
 - We outsourced some of our IT to a third party
 - Is that better than doing it ourselves?
-





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)



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

- Top 10 Nursing Schools in Virginia #3 nurse.org
- The 25 Best Online Bachelor's in Computer Science Programs #5 antiochcollege.net
- 2021 Virginia University Ranking #3 4tu.org
- Find Out the US Universities Without GRE Requirement for Masters #14 youst.com
- Best Universities for Cyber Security in the World #9 edrank.com
- 27 great schools that don't require SAT or ACT scores #12 inredder.com
- Virginia Public Colleges Ranked by Largest Enrollment #2 collegesmely.com
- 50 Best Bachelor's in Sports Science Degree Programs (Campus) #8 sports-management-degrees.com
- The 50 Best Nursing Schools in Virginia #2 nursing-schools-at-mason.com
- Top Colleges for Veterans in the United States #1 collegesforvets.com

About

George Mason University is a public research university in Fairfax County, Virginia. The university was originally founded in 1949 as a southern branch of the University of Virginia. Named after Founding Father of the United States George Mason in 1958, it became an independent university in 1972. Wikipedia

Annual after-tax	Retention rate	Acceptance rate
\$21K	71%	89%

Graduation rate for first-time, full-time undergraduates (more...)
From US Dept of Education: Learn more

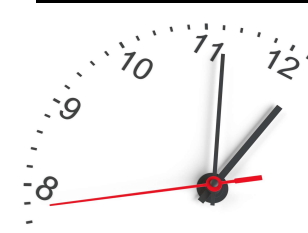
Address: 4400 University Dr, Fairfax, VA 22030
Phone: (703) 993-1000

College's faculty
From US Dept of Education: Learn more

Enrollment 2018-19
25,013 undergraduate students
[More about students](#)

Typical annual income
\$26K
Median income of federal financial aid recipients, 10 years after enrolling at this institution.
[More about outcomes](#)

Average annual in-state cost
In-state fee: \$29,878
Out-of-state: \$21,048
Add in-state 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.

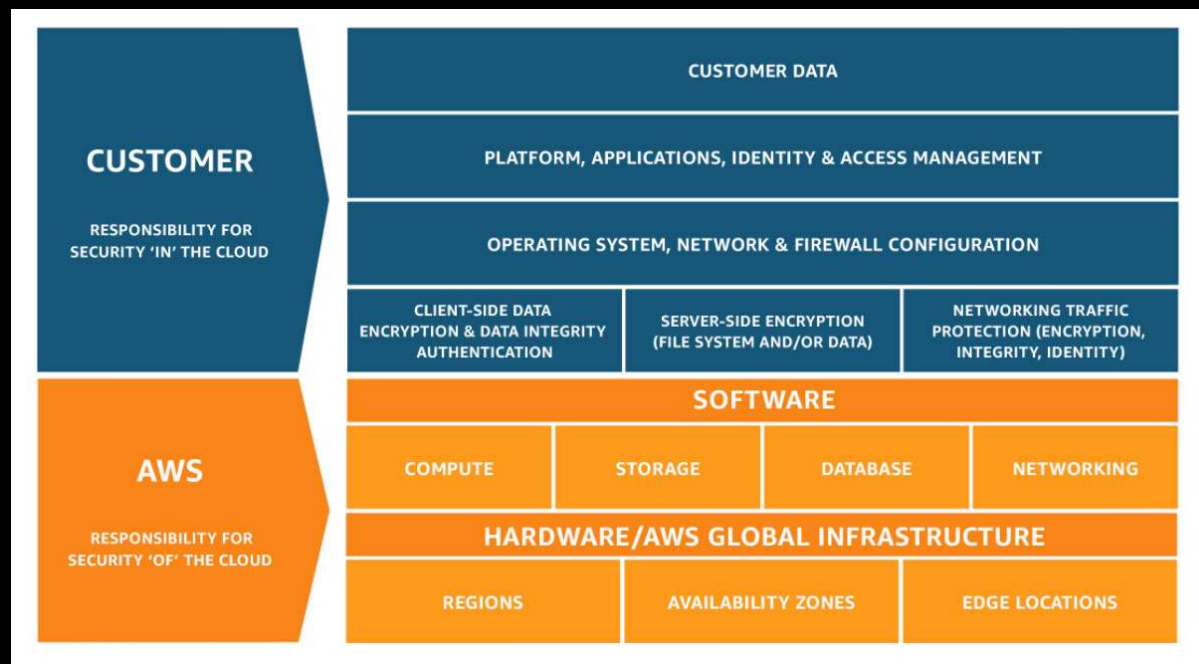
The responsibility changes according to the deployment model

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	Shared	Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Shared	Cloud Provider
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: Blue square = Cloud Customer, Grey square = Cloud Provider

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

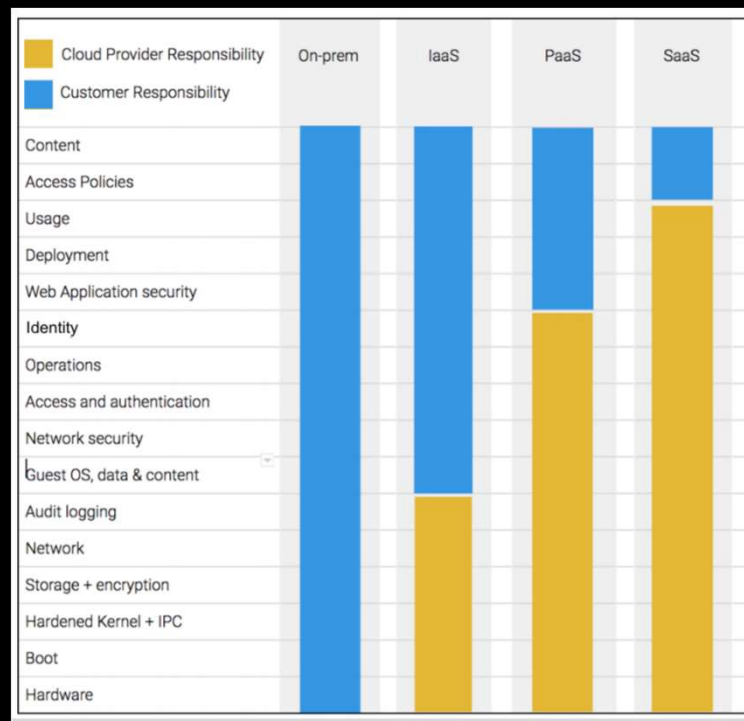
AWS Shared responsibility Model



<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?

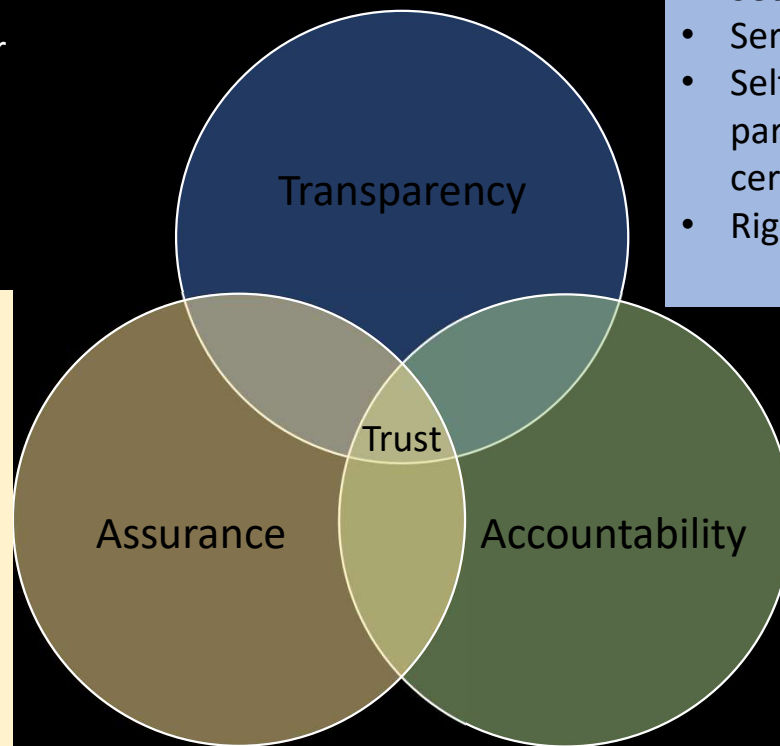
- Everyone has a **role** in the team
 - We all need to **agree** on who is responsible for what
 - This is a supply chain issue
 - One member playing badly could make the other team win
-



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

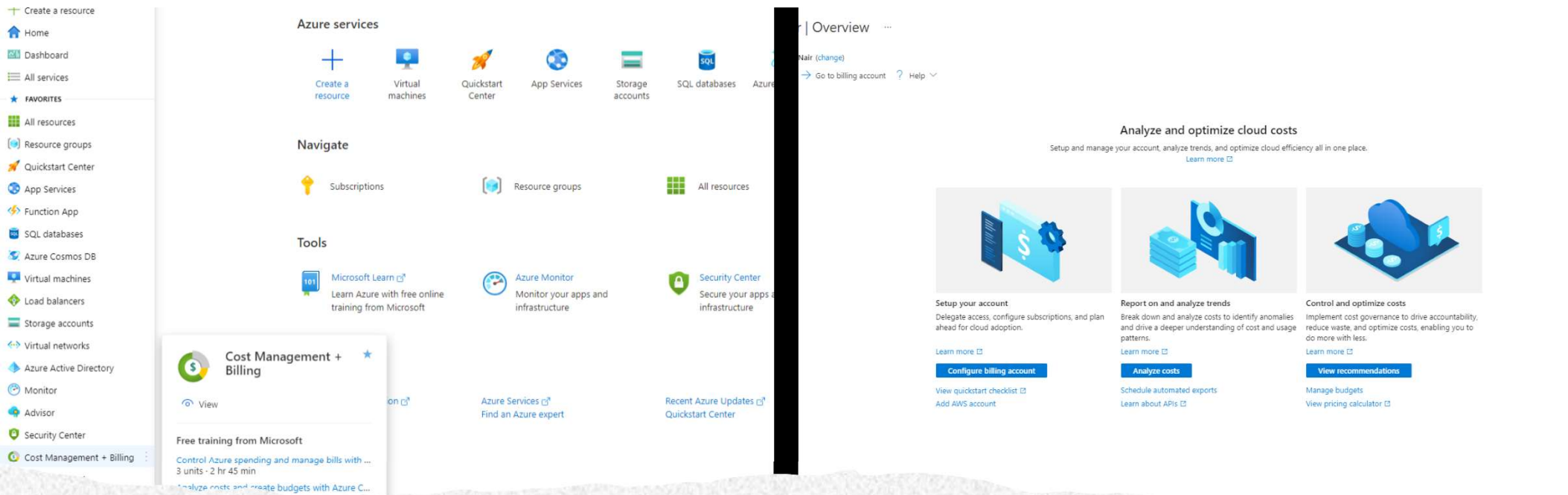
Cost Savings



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 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 subtitle "Configure and estimate the costs for Azure products". A digital display shows the value "07734". Below the heading, there are tabs for Products, Example Scenarios, Saved Estimates, and FAQs. A "Live.com" link and a "Switch Directory" button are also visible. The main content area is titled "Select a product to include in your estimate." and features 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 service cards with icons and descriptions:

- 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.
- Azure Cost Management and Billing**: Manage your cloud spending with confidence.



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

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



Image copyright Google

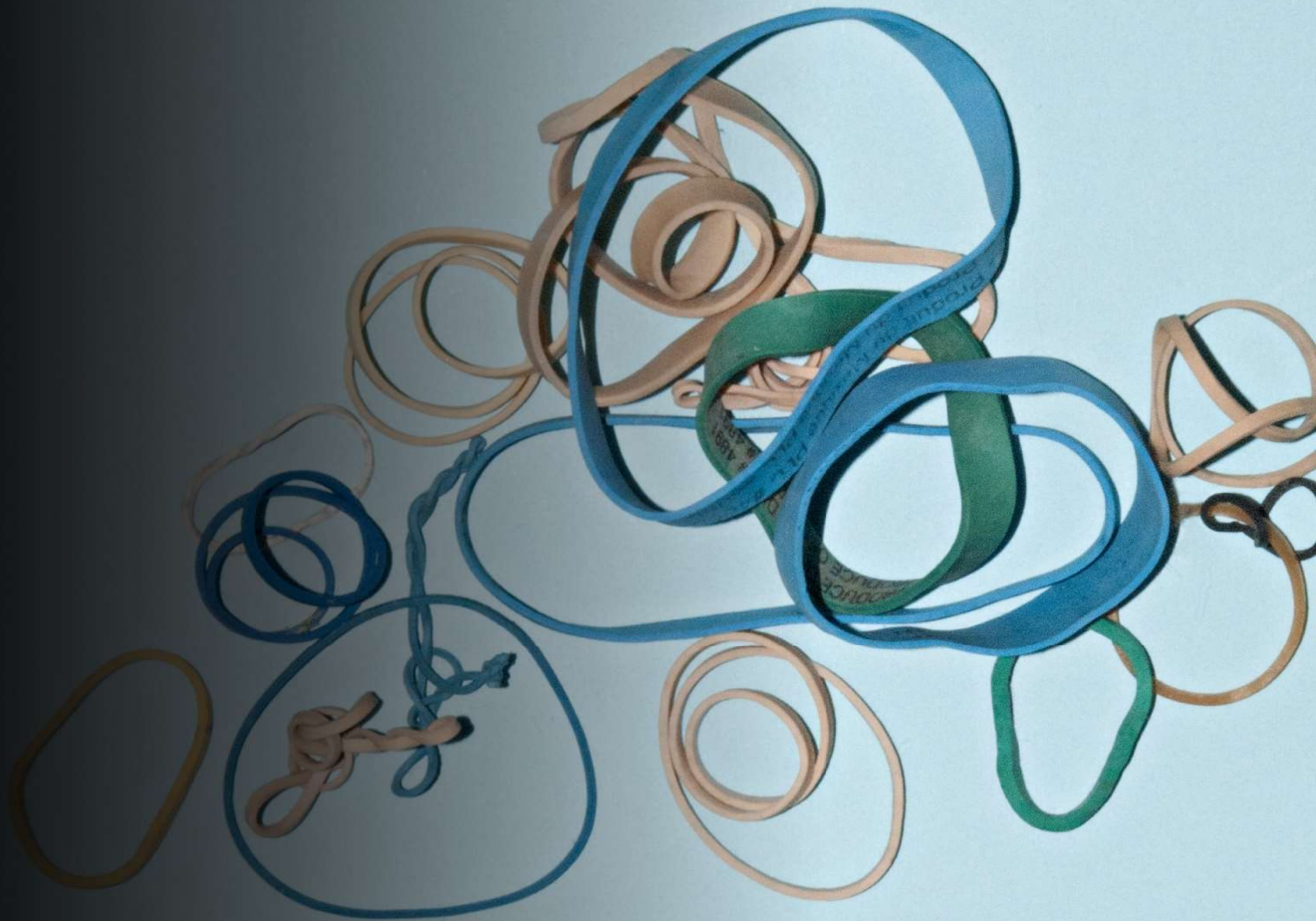
GCP locations are composed of regions and zones.

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.



CLOUD COMPUTING Review

Are these the benefits you are getting from the cloud?

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

- Rearrange this to reflect what benefits caused your company to adopt public cloud. If not, why not?

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
-

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

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

CSA cloud security alliance®

Membership ▾ STAR Program ▾ Certificates & Training ▾ R

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 Ask a p

3DGIS srl

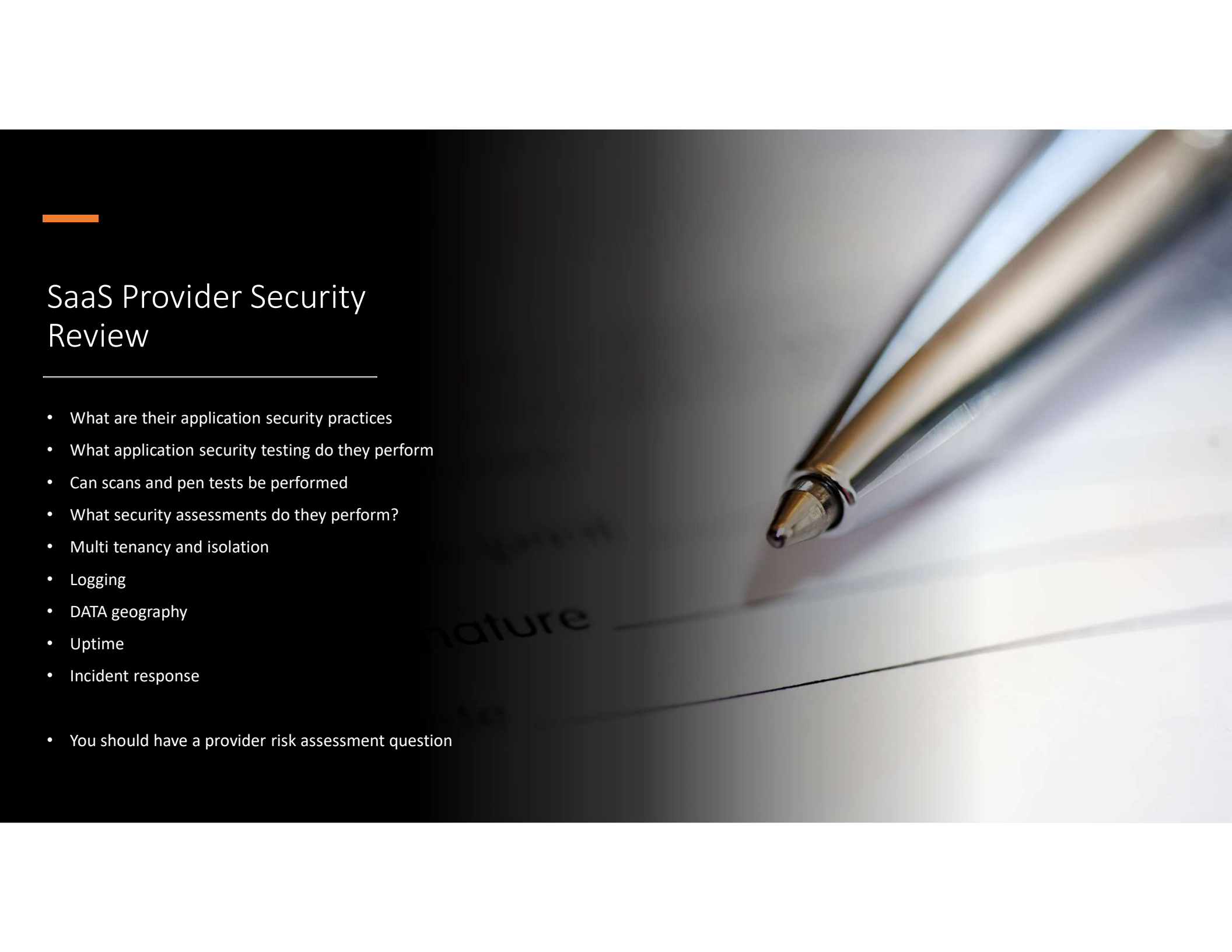
Built on multi-year experience in GeolCT design and GIS development, 3DGIS is a



Demo: CSA STAR

[https://cloudsecurityalliance.org/
star/registry/](https://cloudsecurityalliance.org/star/registry/)





SaaS Provider Security Review

- What are their application security practices
- What application security testing do they perform
- Can scans and pen tests be performed
- What security assessments do they perform?
- Multi tenancy and isolation
- Logging
- DATA geography
- Uptime
- Incident response

- You should have a provider risk assessment question

SaaS risks

01

11% OF SAAS
ACCOUNTS WERE
INACTIVE

02

7 OUT OF 100 USERS
WERE ADMINS

03

80% OF COMPANIES
HAD AT LEAST ONE
FORMER EMPLOYEE
WITH AN ACTIVE
SAAS ACCOUNT

PaaS Security Concerns

Application libraries and configurations

Users

Authentication/Authorization

Encryption

Containers

Containers

OS level
virtualization
Docker is the most
technology for
deploying
containers

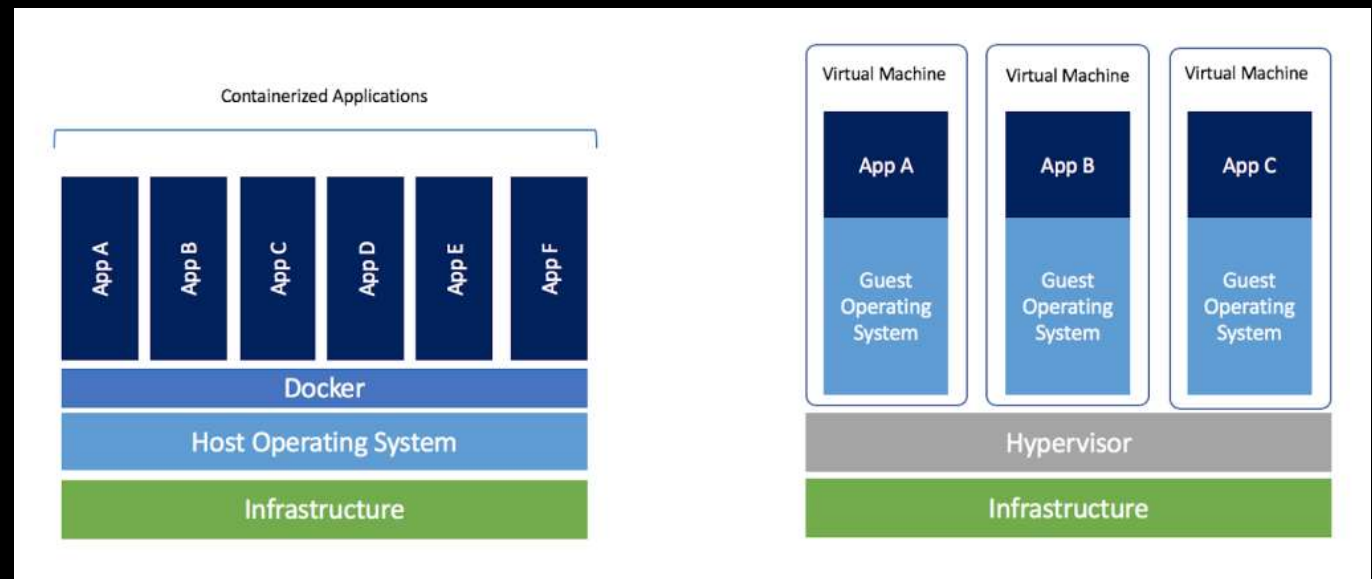
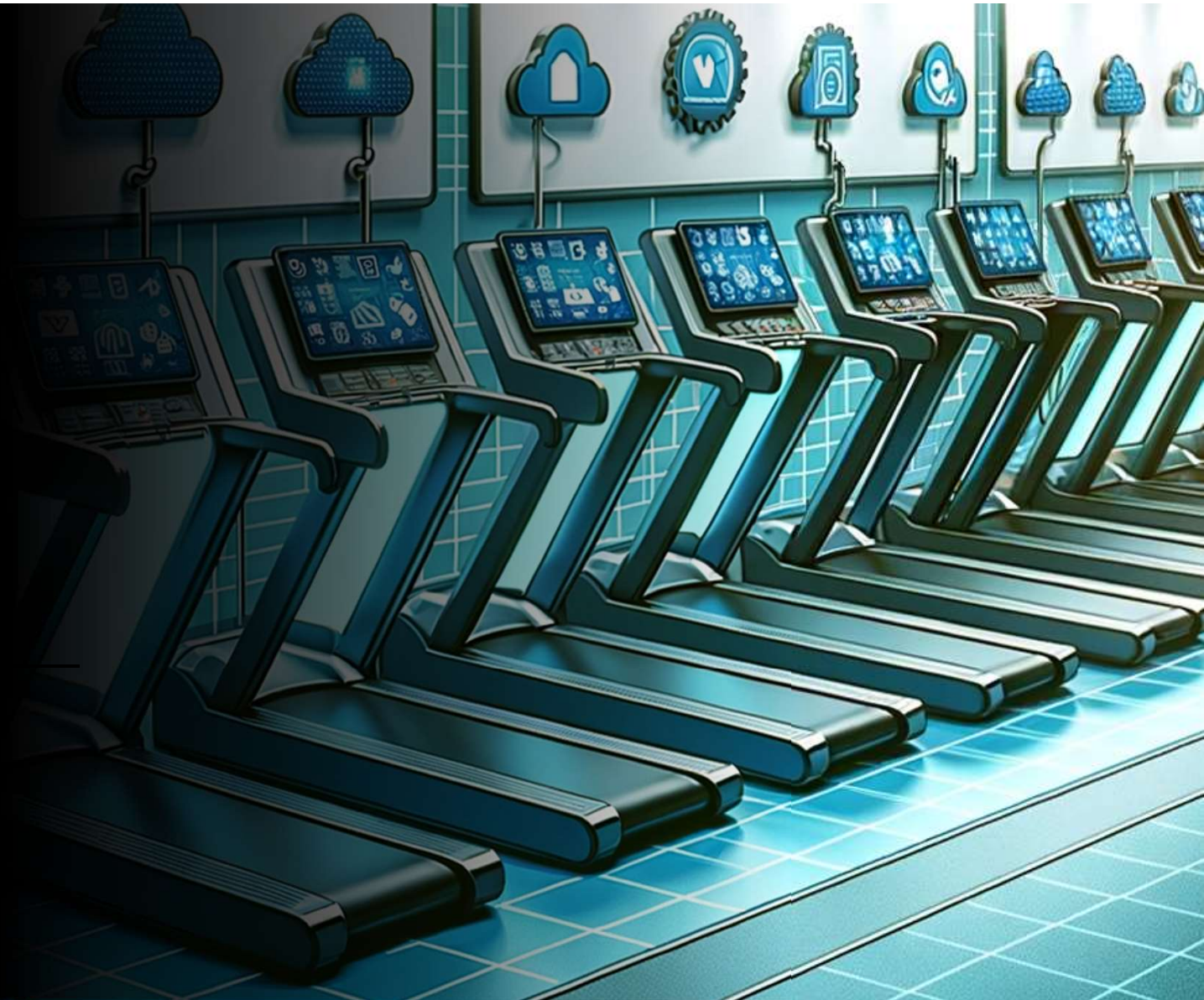


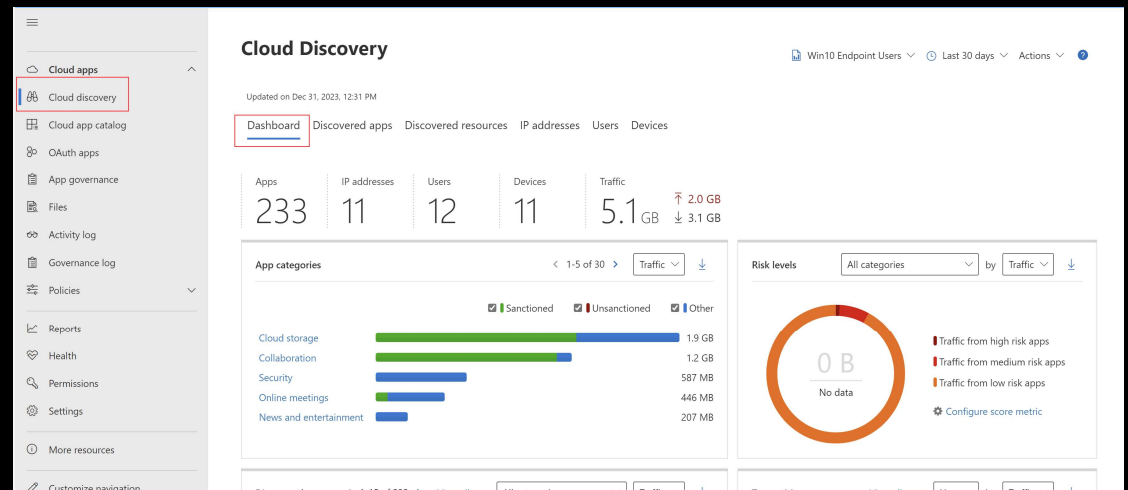
Image from <https://www.docker.com/blog/containers-replacing-virtual-machines/>

Serverless



How do I know what I have in the cloud?

- Cloud Asset Inventory
 - Automated Discovery Tools: Cloud Native or Third Party
- Tagging and Categorization
- CMDB



You can't protect what you can't see



General dashboard

Filter by app: All apps

Alerts

435 open alerts

Over the last 30 days



■ Open ■ Resolved ■ Dismissed

Recent alerts:

Alert	Date
Login from outdated browser...	6/9/20 9:54 AM
Impossible travel activity	6/9/20 9:00 PM
Multiple failed user log on atte...	6/9/20 2:51 PM

[View all alerts](#)

Discovered apps

357 discovered apps

Over the last 30 days



App categories by traffic:



[View all discovered apps](#)

Top users to investigate

145 users to investigate

Investigation priority is calculated using a user's recent activities over the last 7 days

Top users to investigate:

Name
Erni Ruder
Josef Muller Brodmann
Adrian Frutiger
Julie Cooper
Erni Ruder
Josef Muller Brodmann
Adrian Frutiger
Max Medinger

[Investigate users and accounts](#)

Files infected with malware

18 files infected

Identified malicious files in your cloud storage

Recently detected files with malware:

Name

Privileged Office 365 OAuth apps

45 privileged OAuth apps

Privileged apps that users gave permissions to

Most authorized, rarely used privileged OAuth apps:

Name	Authorized by
------	---------------

Azure security configuration

21 Azure recommendations

This assessment, powered by Azure Security Center, provides recommendations for missing configuration and security



Cloud Specific Security Tools

- Cloud Security Posture Management
- Cloud Workload Protection
- Cloud Access Security broker, CASB

How do you securely use the cloud?

The screenshot shows the Microsoft Cloud Adoption Framework for Azure website. The header features the title "Microsoft Cloud Adoption Framework for Azure" and the subtitle "Proven guidance to accelerate your cloud adoption journey". Below the header are two buttons: "Get started" and "Find a partner". A navigation menu includes "Overview", "Cloud adoption journey", "Tools", "Partners", "Resources", and "FAQs". The main content area is titled "What is the Cloud Adoption Framework?" and contains a paragraph explaining the framework's purpose, a second paragraph about its benefits, and a link to "Explore the Framework >". To the right is a video player with the title "Microsoft Cloud Adoption Framework for Azure". The footer contains three columns of content, each with an icon, a title, and a brief description.

Microsoft Cloud Adoption Framework for Azure
Proven guidance to accelerate your cloud adoption journey

[Get started](#) [Find a partner](#)

[Overview](#) [Cloud adoption journey](#) [Tools](#) [Partners](#) [Resources](#) [FAQs](#)




What is the Cloud Adoption Framework?

The Cloud Adoption Framework is proven guidance that's designed to help you create and implement the business and technology strategies necessary for your organization to succeed in the cloud. It provides best practices, documentation, and tools that cloud architects, IT professionals, and business decision makers need to successfully achieve their short- and long-term objectives.

By using Cloud Adoption Framework best practices, organizations are better able to align their business and technical strategies to ensure success.

[Explore the Framework >](#)

Microsoft Cloud Adoption Framework for Azure

- **Realize your business objectives**
Identify opportunities for your organization in the cloud and realize your objectives using cloud technology.
- **Prepare your organization for the cloud**
Identify productive and sustainable ways to help your organization understand and embrace technology changes that will improve business outcomes.
- **Migrate to the cloud and optimize**
Move your digital assets to the cloud and then optimize them—and your operational processes—for excellence with innovative cloud-based technologies.

<https://azure.microsoft.com/en-us/cloud-adoption-framework/> - Azure

<https://cloud.google.com/adoption-framework/> - GCP

<https://aws.amazon.com/professional-services/CAF/> - AWS



Demonstration of the Cloud Adoption Site

- [Tools and templates - Cloud Adoption Framework | Microsoft Docs](#)
- <https://aws.amazon.com/professional-services/CAF/>



Certificate of Cloud Auditing Knowledge

- Demonstrate your capability to audit the cloud

The screenshot shows a web browser window displaying the ISACA Greater Washington, D.C. Chapter website. The page features a navigation menu with links for Home, About, Contact Us, Membership, Events, Event Replays, News & Articles, Certifications, One In Tech, and Sponsor Us. The main content area highlights a "Certificate of Cloud Auditing Knowledge (CCAK™) Review Course" scheduled for March 18 @ 8:30 am - March 26 @ 5:00 pm EDT. The course is sponsored by GWDC, with a fee of \$400 for members and \$800 for non-members. A green button labeled "Register today!" is prominently displayed. The page also includes social media icons and a "Subscribe" button.

ing-review/

Presentations ▾ Job Opportunities Volunteer ▾ FAQs Visit ISACA.org

ISACA
Greater Washington, D.C. Chapter

Subscribe Join ISACA CPE Questions

Home About Contact Us Membership Events Event Replays News & Articles Certifications One In Tech Sponsor Us

« All Events

Certificate of Cloud Auditing Knowledge (CCAK™) Review Course

March 18 @ 8:30 am - March 26 @ 5:00 pm EDT GWDC Member \$400, Non-GWDC Member \$800

« CISM Spring 2022 Review Course CISA Spring 2022 Review Course »

The GWDC is sponsoring an intensive 4-day review course for the Certificate of Cloud Auditing Knowledge (CCAK™). The dates of this course are **March 18 -19 and 25 - 26, 2022** from 8:30 am to 5:00 PM Eastern. Please **register by March 15!**

[Register today!](#)

The course will provide knowledge on cloud security assessment methods and techniques, and will assist students in updating their expertise in cloud and hybrid security auditing. CCAK is a joint project by Cloud Security Alliance® and ISACA®. The CCAK is the first credential available for industry professionals to demonstrate their expertise in the essential principles of auditing cloud computing systems. The CCAK credential and training program fills the gap in the market for technical education for cloud IT auditing.

The CCAK course is designed to cover the following five core areas of focus: Cloud governance, Cloud compliance, Cloud auditing, Cloud assurance, and CSA tools.

CSA References

Cloud Controls Matrix (CCM)

Consensus Assessment Initiative Questionnaire (CAIQ) v4

Guidance for critical areas of focus in cloud computing

Open Certification Framework

Privacy Level Agreement

GDPR Code of Conduct

Cloud enterprise architecture

Software Defined Perimeter

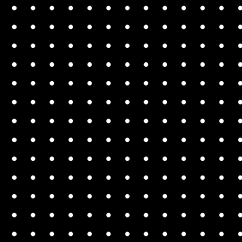
Learning more about cybersecurity and Cloud

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





Thank you



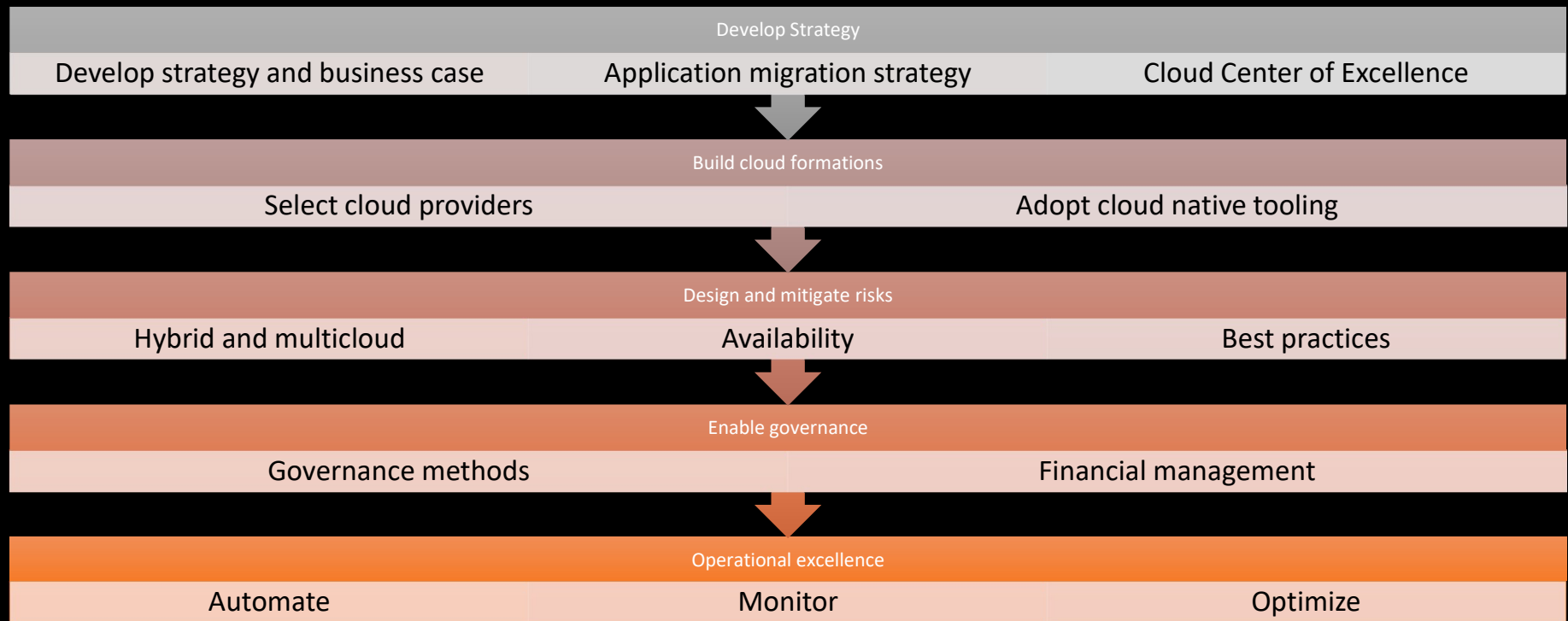
- Any questions???
- Contact nairsushi@gmail.com
- Follow me on LinkedIn
<https://www.linkedin.com/in/sushilanair/>
- Twitter [@sushila_nair](https://twitter.com/sushila_nair)

Community builds our skills and network

The background of the page is a complex marbled paper pattern. It features intricate, swirling lines in shades of deep red, forest green, and black, creating a rich, textured appearance. The colors are interwoven in a way that suggests organic, fluid movement.

Appendix

Public Cloud Adoption Framework





1. Develop Strategy

- Develop strategy and business case
- Application migration strategy
- Cloud Center of Excellence

Cloud Strategy



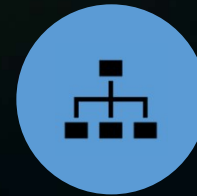
EXECUTIVE
SUMMARY



OBJECTIVES



RISKS



ORGANIZATIONAL
IMPACT



KEY ADOPTION
PRINCIPLES

Cloud Strategy Document

Services strategy

When to consume

When to build

How to secure

Principles

Cloud first?

Multi cloud or single cloud

Migrate workload by workload or lift and shift

Security

Governance, compliance and privacy

Exit

Getting data back

Contracts

Development and architectural issues

A cloud strategy is a set of choices and decisions that will allow an organization to adopt cloud and align the adoptions to the business objectives

Application Migration Strategy

- Rehosting (lift-and-shift)
- Replatforming
- Repurchasing
- Refactoring / Re-architecting
- Retire
- Retain

Cloud Center of Excellence

A CCOE provides central IT with a way to express the CIO's cloud strategy and provide governance through policies and cloud management tools, as well as gather and disseminate cloud best practices

- Governance – Policies and Governance tools
- Brokerage: Assist users in selecting cloud providers, architect the cloud solution(s) and collaborate with the sourcing team for contract negotiation and vendor management.
- Community: Raise the level of cloud knowledge in the organization and capture and disseminate best practices through a knowledge base, source code repository, training events, outreach throughout the organization, and more.



Discussion

- How do you create a talent pipeline for cloud?
- What training methodologies do you think best help build organizational skills?
- How do you handle a skills shortage?



A young girl with long brown hair, wearing safety goggles and a red and black plaid shirt, is focused on working on a project. She is using a pair of white-handled pliers to work on a component on a table. In the background, there is a whiteboard with a blue and white circular diagram and some other lab equipment. The lighting is soft and focused on her work area.

2. Build Cloud Formations

- Select cloud providers
- Adopt cloud native tooling

Select Cloud Providers

Business health
and processes

Administration
support

Technical
capabilities &
Roadmap Security
Practices

Certifications &
Standards

Data Security, Data
Governance and
Business policies

Service
Dependencies &
Partnerships

Contracts,
Commercials &
SLAs

Reliability &
Performance

Migration Support,
Vendor Lock in &
Exit Planning

Cloud provider audits

Reviewable audits

- Scope and time
- Service coverage
- Audit Firm History





Tools

- Cloud Native
- CSP Native
- Born in the cloud


Influencers

- Licensing
- Best of Breed vs Platform
- Born in the cloud

Cloud Native Tooling

- Amazon Web Services (AWS) is the world's most broadly adopted cloud platform, offering **over 200 fully featured services** from data centers globally.
- The Azure cloud platform has **more than 200 products** and cloud services designed to help you bring new solutions to life





3. Design and Mitigate Risk

- Hybrid and multicloud
- Availability
- Best Practices



Cloud Landing Zones

- A landing zone is the underlying core configuration of any cloud adoption environment.
- Landing zones provide a pre-configured environment - provisioned through code - to host workloads in private, hybrid, or public clouds.
- Here are 4 key aspects a landing zone can and should take care of in your cloud:
 - Security & Compliance
 - Standardized tenancy
 - Identity and access management
 - Networking





How to create a cloud landing zone

- Microsoft Azure: Implemented in the Cloud Adoption Framework. Azure blueprints allow you to choose and configure the landing zone blueprints Azure to set up your cloud environments. As an alternative, you can use third-party services like terraform.
- Amazon Web Services: Implemented as AWS Landing Zone. This solution includes a security baseline pre-configuring AWS services like CloudTrail, GuardDuty, and Landing Zone Notifications. The service also automates the setup of a landing zone environment thereby speeding up cloud migrations. AWS offers Cloud Formation Templates to customize and standardize service or application architectures.
- Google Cloud Platform: Google Deployment Manager allows the use of flexible template and configuration files leveraging Yaml - or Python and Jinja2 templates to configure deployments.

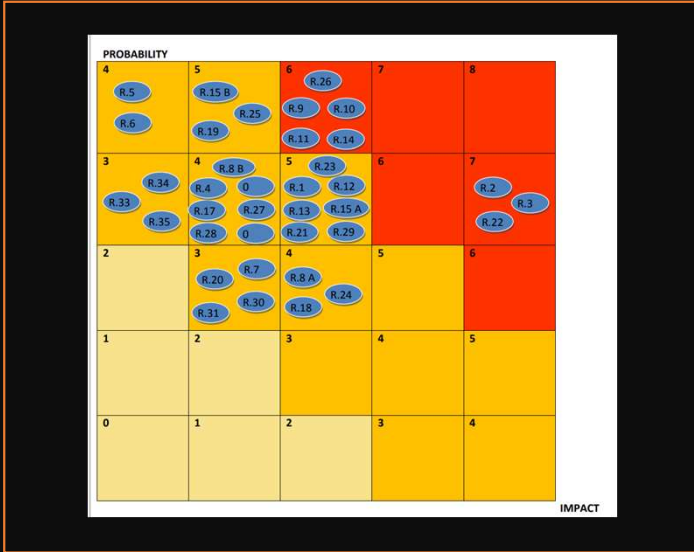


Cloud Risks

- There is less physical control over assets and their controls and processes
- There is a greater reliance on contracts, audits, and assessments, as you lack day-to-day visibility or management.
- Cloud providers also constantly evolve their products and services to remain competitive and these ongoing innovations might exceed, strain, or not be covered by existing agreements and assessments.
- Cloud customers have a reduced need (and associated reduction in costs) to manage risks that the cloud provider accepts under the shared responsibility model.
- Enterprise Risk Management, ERM relies on good contracts and documentation to know where the division of responsibilities and potential for untreated risk lie.

Cloud Security risk assessment Guidance

- The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact.
- The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.



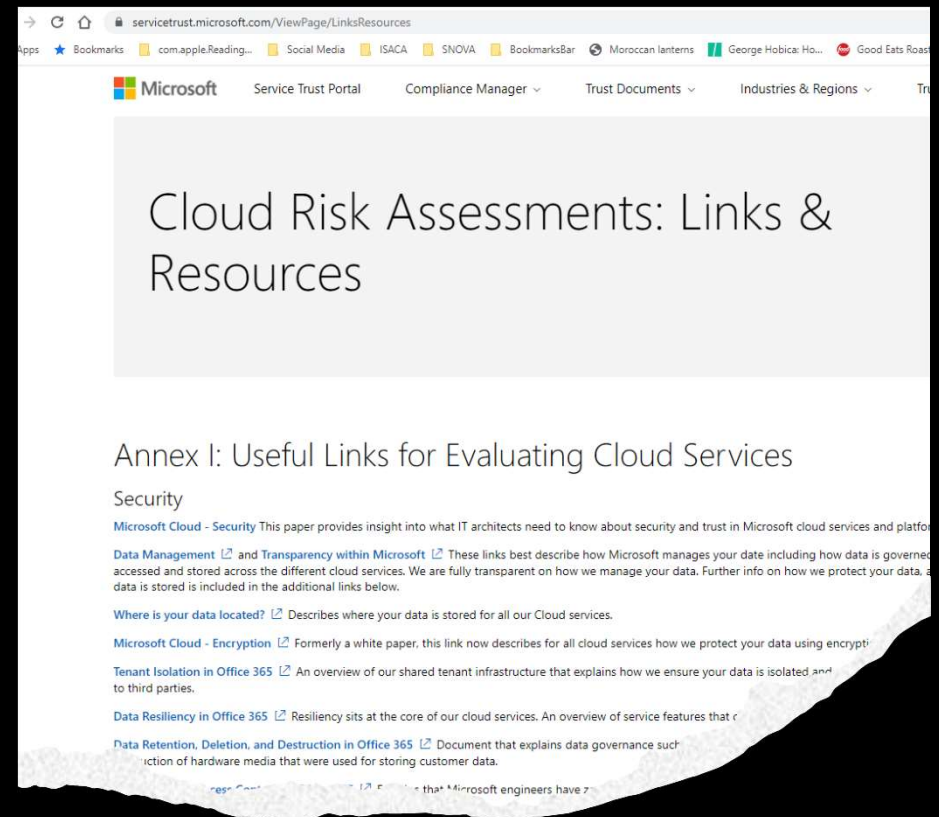
Low risk: 0-2
 Medium Risk: 3-5
 High Risk: 6-8

POLICY AND ORGANIZATIONAL RISKS		
R.1 Lock-in		
Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	HIGH	
<p>There is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability (although some initiatives do exist, e.g., see. (58)). This makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment. Furthermore, cloud providers may have an incentive to prevent (directly or indirectly) the portability of their customers services and data.</p>		

Cloud Risk

resources

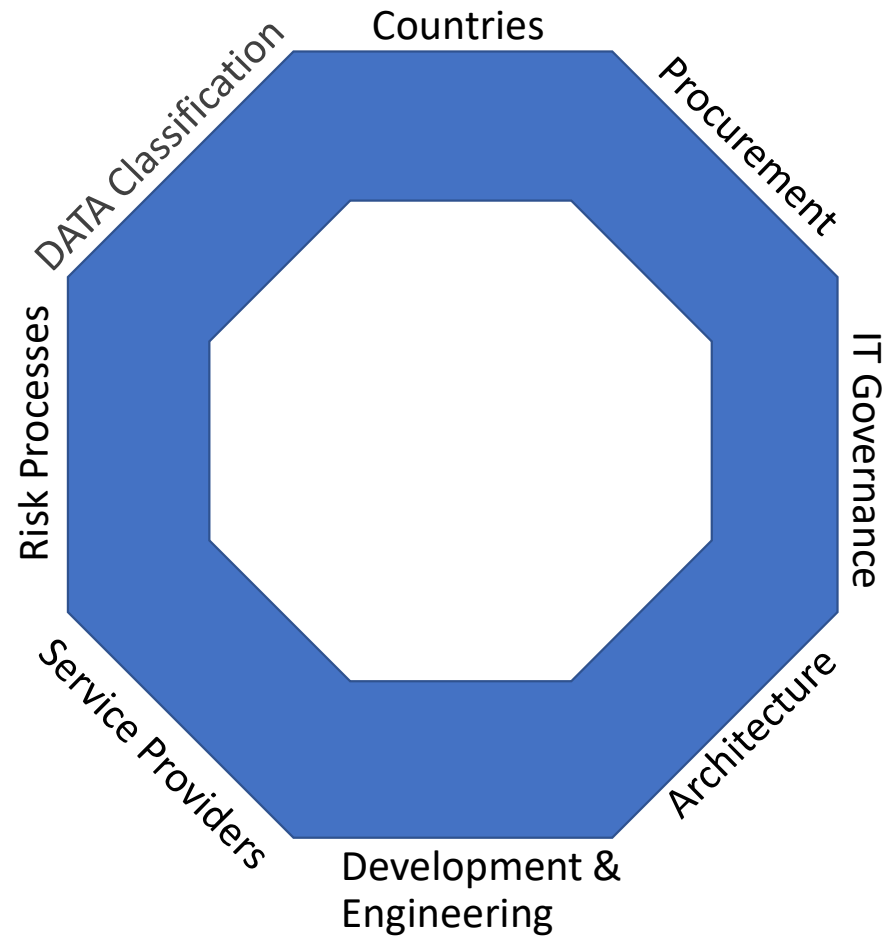
<https://servicetrust.microsoft.com/ViewPage/LinksResources>



The screenshot shows a web browser window displaying the Microsoft Service Trust Portal. The page title is "Cloud Risk Assessments: Links & Resources". The navigation bar includes "Microsoft", "Service Trust Portal", "Compliance Manager", "Trust Documents", and "Industries & Regions". The main content area features a section titled "Annex I: Useful Links for Evaluating Cloud Services" with a sub-section for "Security". Below this, there are several links with brief descriptions:

- [Microsoft Cloud - Security](#): This paper provides insight into what IT architects need to know about security and trust in Microsoft cloud services and platform.
- [Data Management](#) and [Transparency within Microsoft](#): These links best describe how Microsoft manages your data including how data is governed, accessed and stored across the different cloud services. We are fully transparent on how we manage your data. Further info on how we protect your data, and how your data is stored is included in the additional links below.
- [Where is your data located?](#): Describes where your data is stored for all our Cloud services.
- [Microsoft Cloud - Encryption](#): Formerly a white paper, this link now describes for all cloud services how we protect your data using encryption.
- [Tenant Isolation in Office 365](#): An overview of our shared tenant infrastructure that explains how we ensure your data is isolated and protected from access to third parties.
- [Data Resiliency in Office 365](#): Resiliency sits at the core of our cloud services. An overview of service features that ensure your data is protected and available.
- [Data Retention, Deletion, and Destruction in Office 365](#): Document that explains data governance such as retention of hardware media that were used for storing customer data.

Cloud Octagon Model





4. Enable Governance

- Governance methods
- Financial Management



Discussion

Why is governance impacted using cloud compared to on premise?

What challenges does cloud bring which is different from a 100% on premise architecture?



The primary tool of governance is the contract between a cloud provider and a cloud customer



Five disciplines of cloud governance

Cost Management

- Evaluate & monitor cost. Create cost accountability

Security Baseline

- Apply a security baseline

Resource Consistency

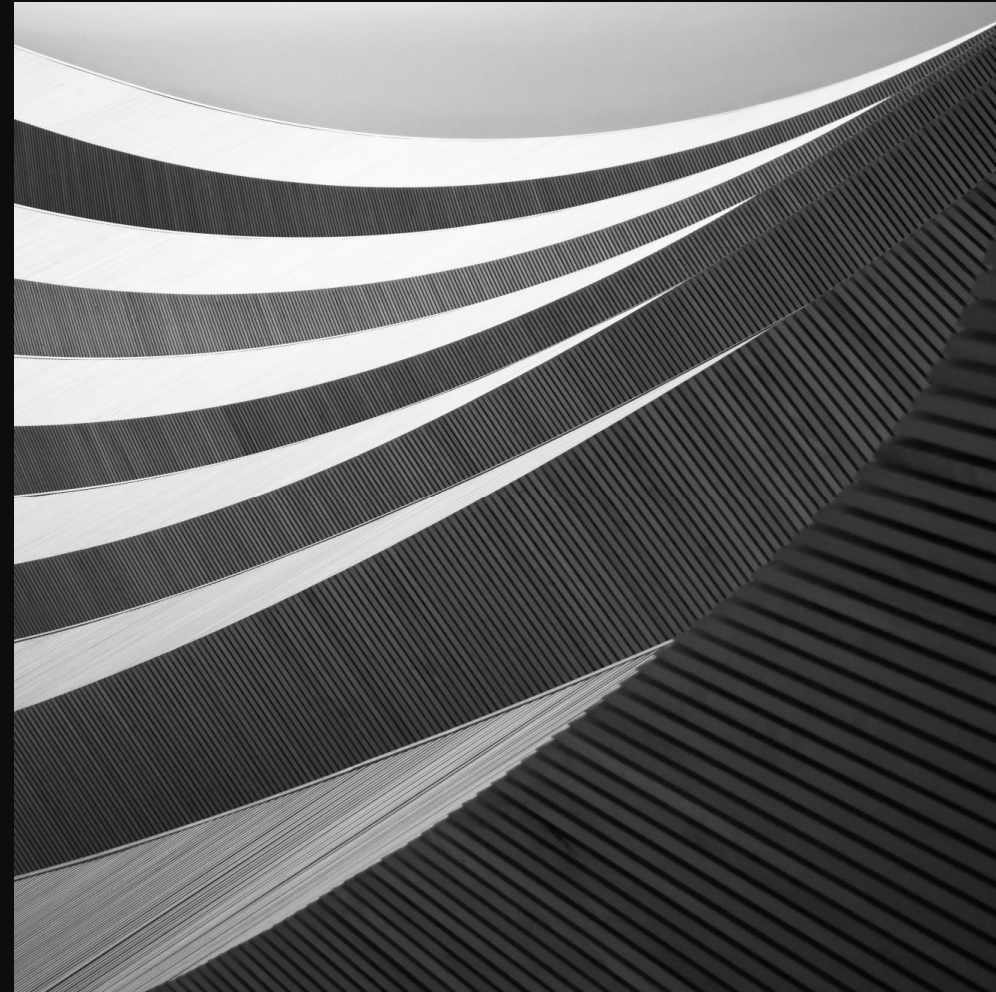
- Ensure consistency in resource configuration

Identity Baseline

- Consistently apply role definitions and assignments

Deployment Acceleration

- Centralization consistency to enable accelerated deployment
-



5. Operational Excellence

- Automate
 - Monitor
 - Optimize
-





Discussion

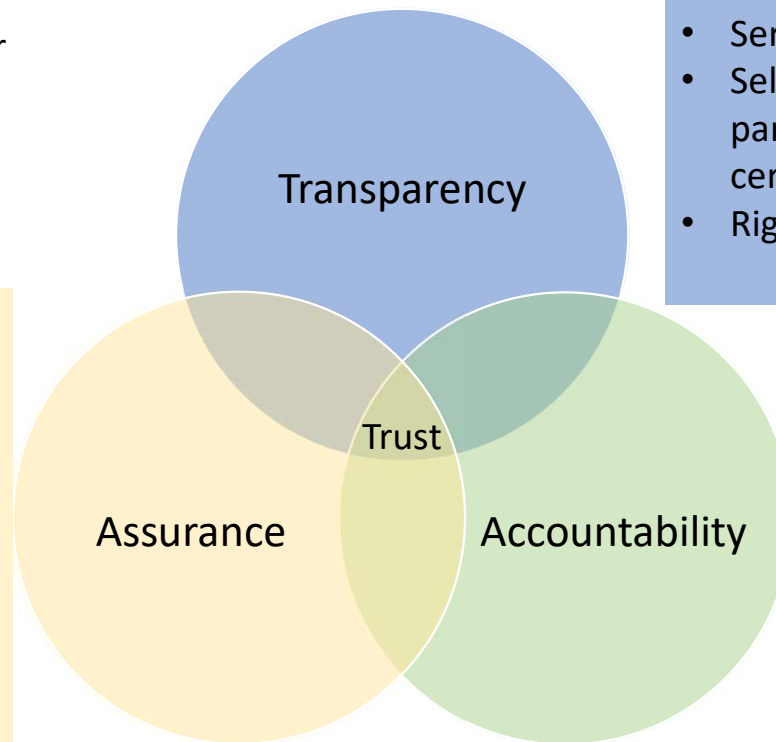
- How and why do you automate in the cloud?
- How do you monitor the events in the cloud?
- How do you optimize your cloud operations?



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



Membership ▾

STAR Program ▾

Certificates & Training ▾

R

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

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.

Submi
Ask a p



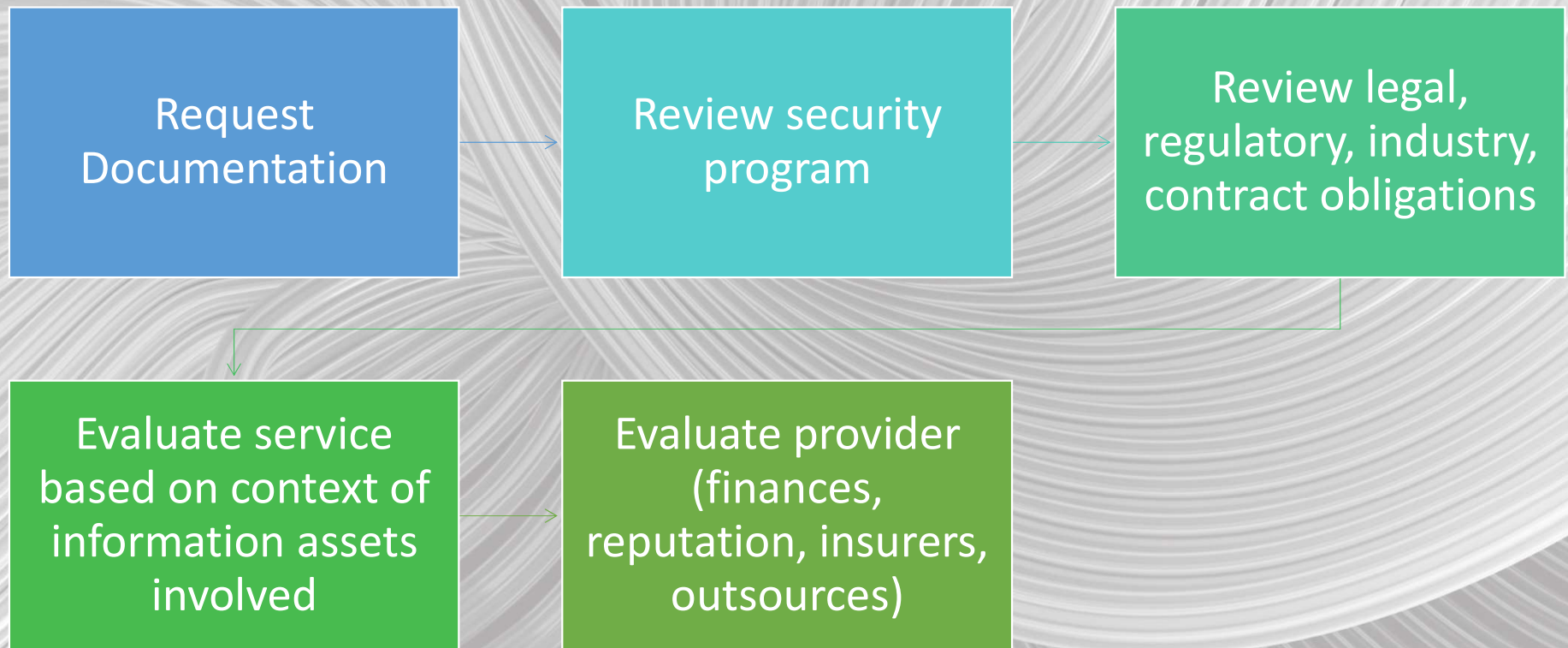
Filter Your Results ▲

3DGIS srl

Built on multi-year experience in GeoICT design and GIS development, 3DGIS is a melting pot of computer science.

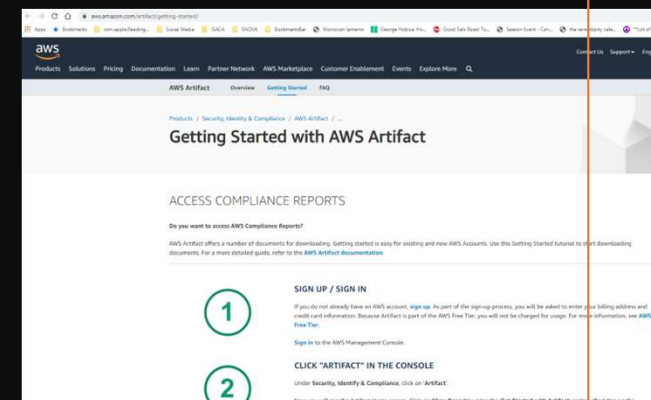
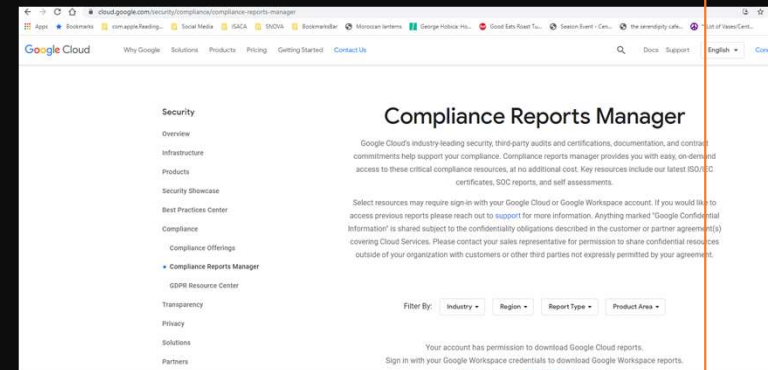
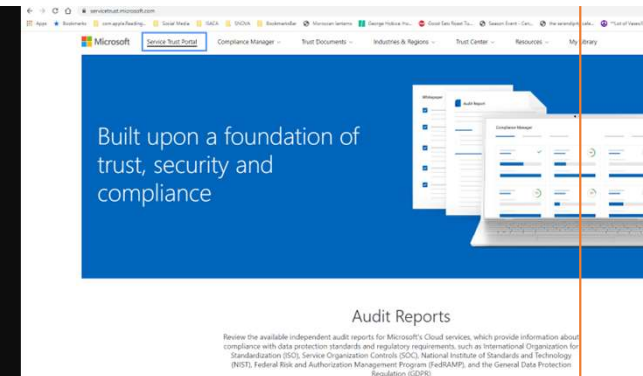


Reminder – This documentation is used for cloud provider selection and ongoing assessment



Accessing CSP audit reports

- GCP compliance report manager
- MS service trust portal
- AWS Artifact



Demonstration on Microsoft

- <https://servicetrust.microsoft.com/>
 - Download Office 365 Central - SOC 2 Report
 - Download Independent vulnerability assessment of M365 carried out 2020.

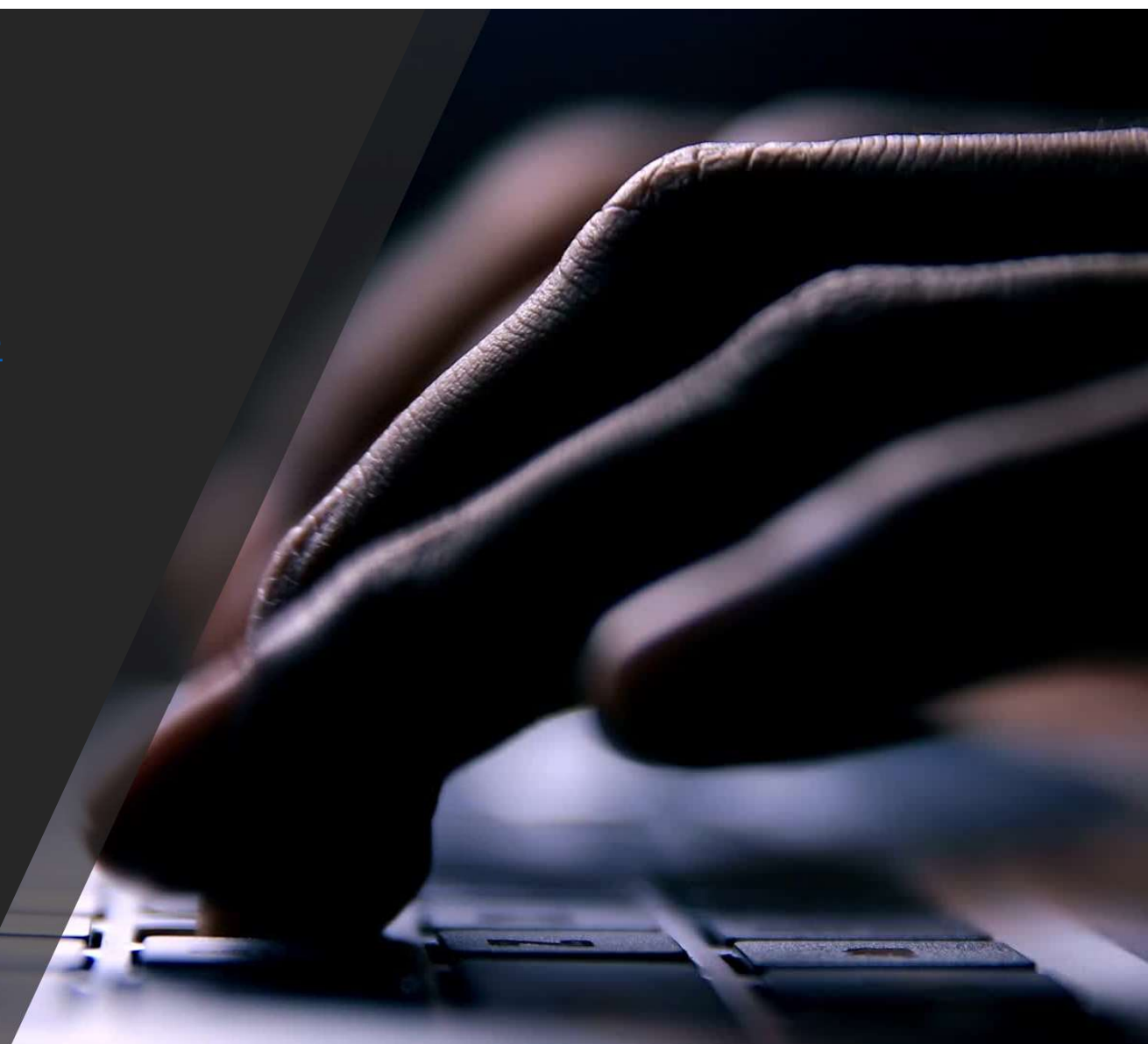


Match the definitions and terms

- Cloud assurance
 - Cloud security
 - Cloud compliance
 - Cloud privacy and control
 - Cloud trust
-
- is having certainty in the security, compliance, transparency, and privacy of the cloud system housing your data.
 - ensure that customers own their data, which can only be accessed, used, deleted, and shared as determined by the customer
 - can be defined as ensuring security, compliance, privacy, and trust in cloud services so that the services are functioning as intended. Simply put, customers want cloud service providers to do the right thing—and to prove it.
 - entails the security measures in place so that a system meets specific requirements defined in standards, regulations, and policies
 - is comprised of the architectural and operational foundation and processes in place to safeguard a physical and virtual system as well as the data and functions that it hosts.

Hands on AWS

<https://aws.amazon.com/artifact/getting-started/> (Needs a AWS free tier account)

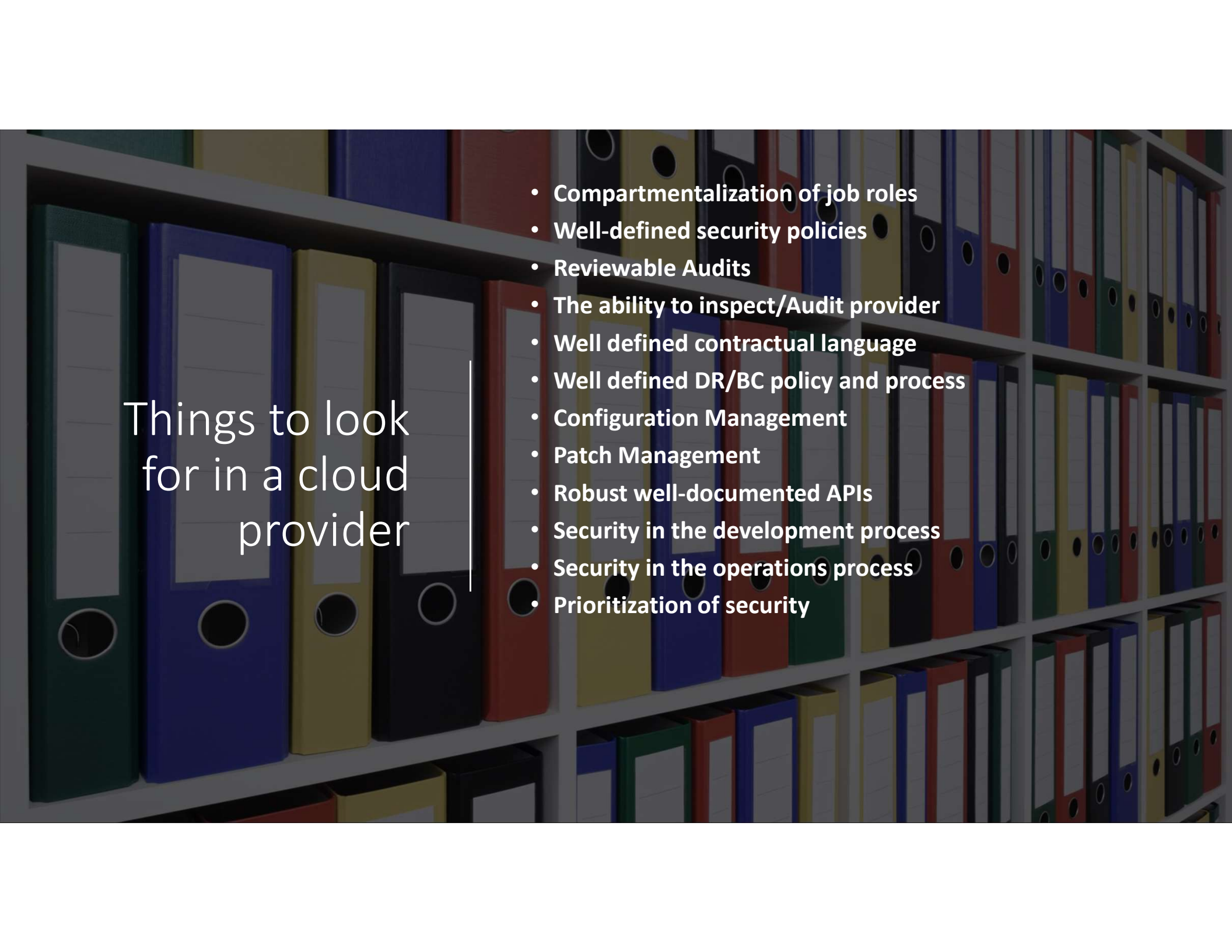


Hands on GCP

- Download PCI-DSS v3.2 audit report
- What GCP services are FedRAMP High?

<https://cloud.google.com/security/compliance/compliance-reports-manager>





Things to look for in a cloud provider

- **Compartmentalization of job roles**
- **Well-defined security policies**
- **Reviewable Audits**
- **The ability to inspect/Audit provider**
- **Well defined contractual language**
- **Well defined DR/BC policy and process**
- **Configuration Management**
- **Patch Management**
- **Robust well-documented APIs**
- **Security in the development process**
- **Security in the operations process**
- **Prioritization of security**

Suggested
Labs you can
complete on
your own

- Azure Fundamentals
- <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/>
- AWS Fundamentals
- [AWS Fundamentals - Core Concepts \(amazon.com\)](https://aws.amazon.com/fundamentals/core-concepts/)
- GCP Fundamentals
- https://google.qwiklabs.com/course_templates/153?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A1%2C%22has_search%22%3Afalse%7D