Risk Revolution

Cybersecurity and Auditing in the Age of Disruption

Who am I?

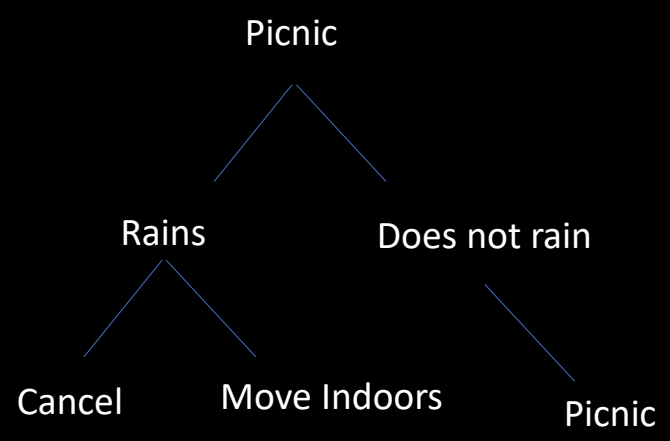
- Security Evangelist
- ISACA emerging trends working group & VP at ISACA GWDC
- 25 years in cyber including 10 years as a CISO
- CISSP,CCAK,CCSK,CRISC,CISA,CISM, CDPSE, GIAC

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

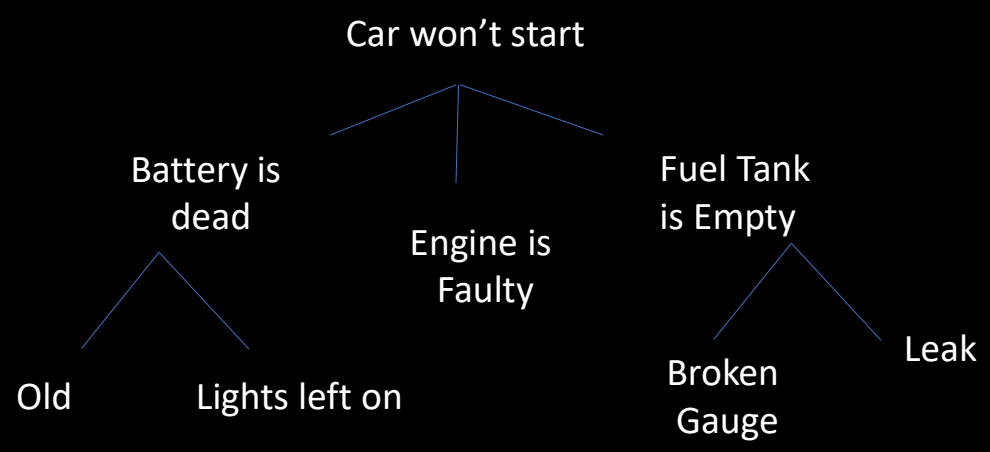
– Choose 2 events that could have caused it and build it from there

Why is this valuable?

Event Tree

```
                Ransomware Attack
                    /      \
                   /        \
                  /          \
          Phishing Email    Exploit
             /     \        /     \
            /       \      /       \
     Click Link   Malicious    Software
                     File     Vulnerability
```

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

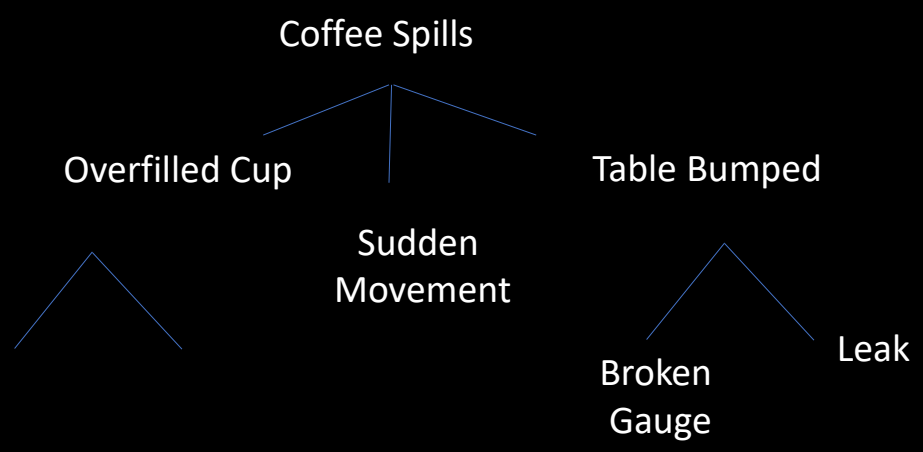
– Choose 2 events that could have caused it and build it from there

Why is this valuable?

Fault tree

```
            Ransomware Attack
                /   \
               /     \
              /       \
        Phishing    Exploit
        Failure      Failure
         /            \
        /              \
Email Filtering     Software Patching
 Failure              Failure
```

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

```
                    Ransomware Attack
                          |
              ------------------------------
             |                              |
      Phishing Email                   Exploit
             |                              |
     ---------------                ----------------
    |               |              |                |
Email Filtering Failure    Software Patching Failure
    |                              |
------------------           ------------------
|                |           |                |
Click Link      Malicious   Vulnerability  Ransomware Deployment
                  File
```

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

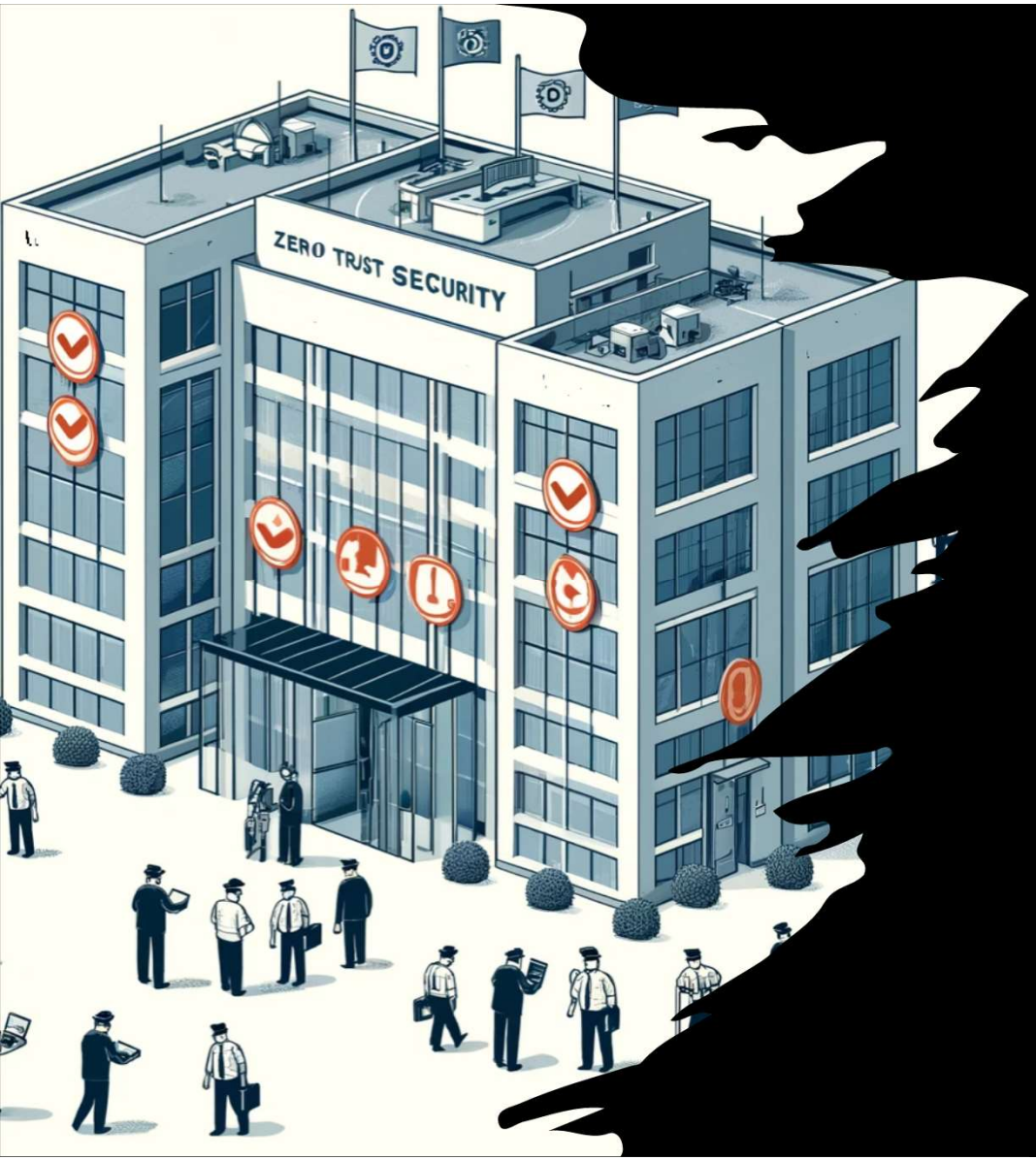
Door

Outdoor Camera $1,000

Cloud based storage for video recording $500 per year

Provide labels here for any symbols you use!

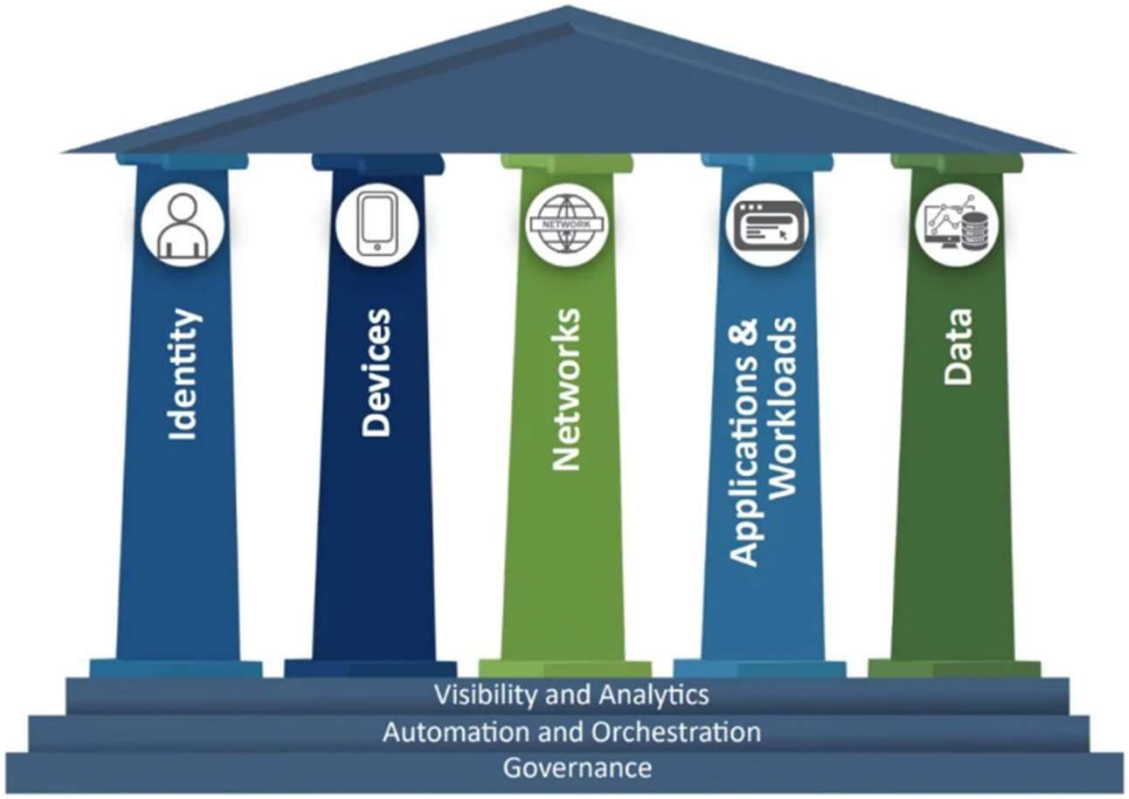
Zero Trust



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**

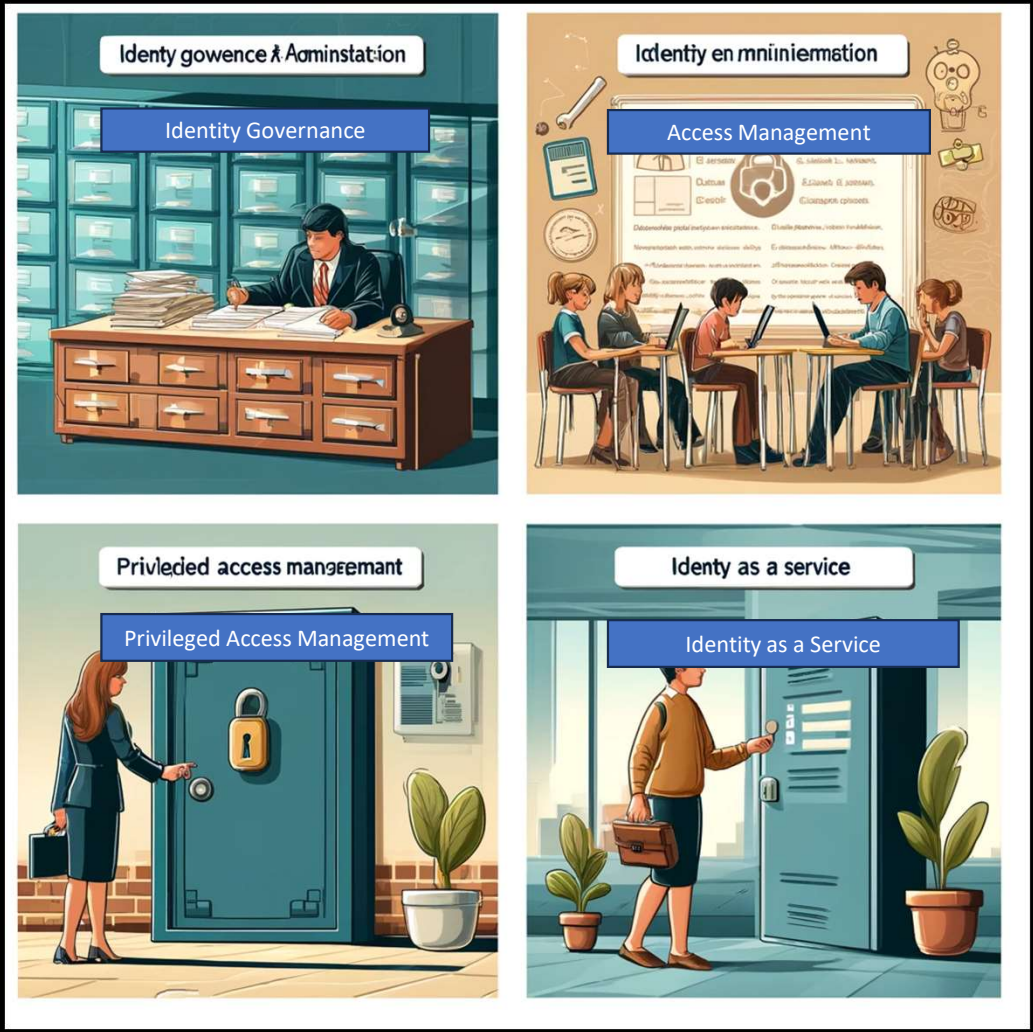
Allowed

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

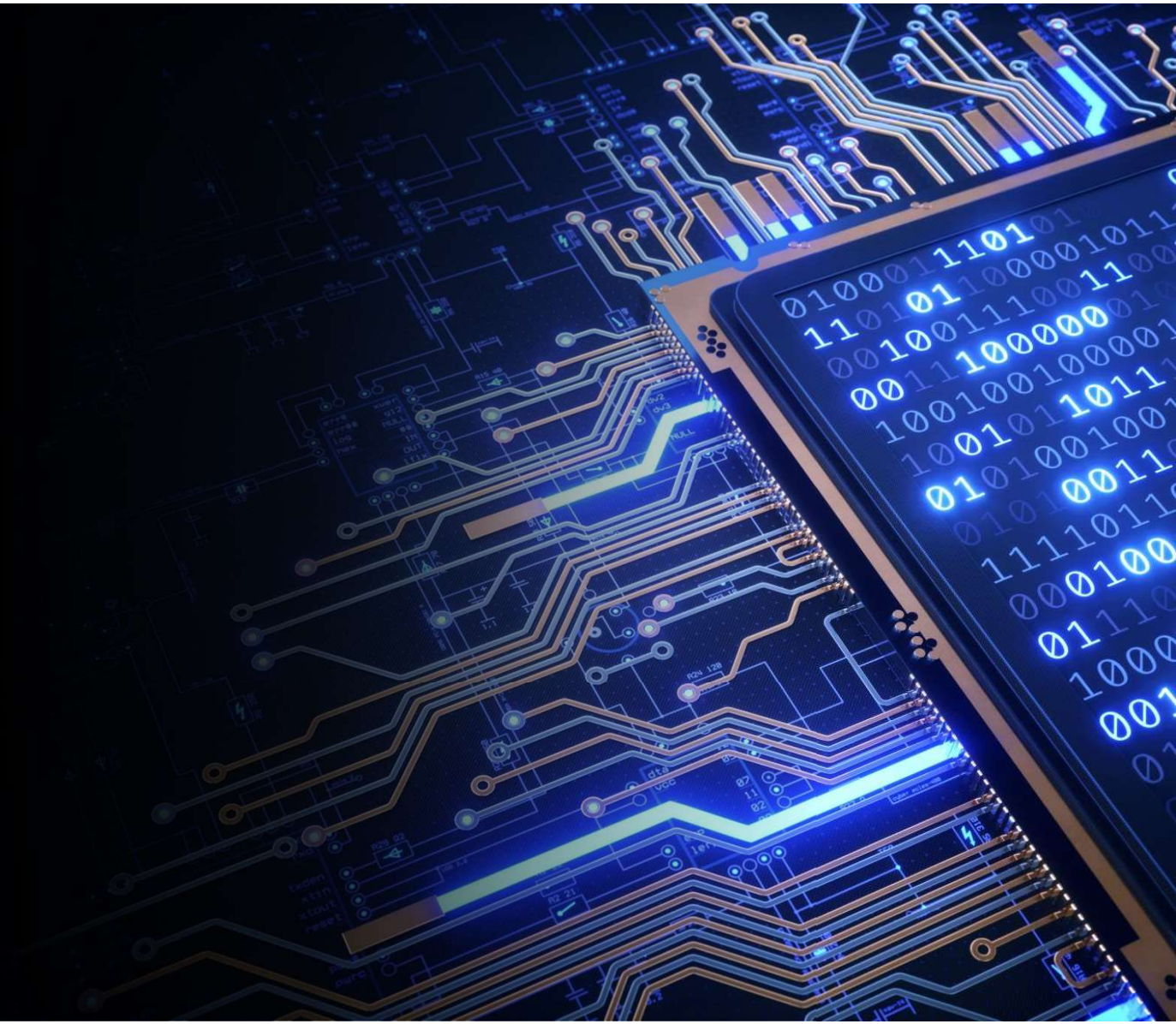
Device Security Posture Assessment

Device Health and Integrity

Secure Device Management

Least Privilege Access

Continuous Monitoring and Logging



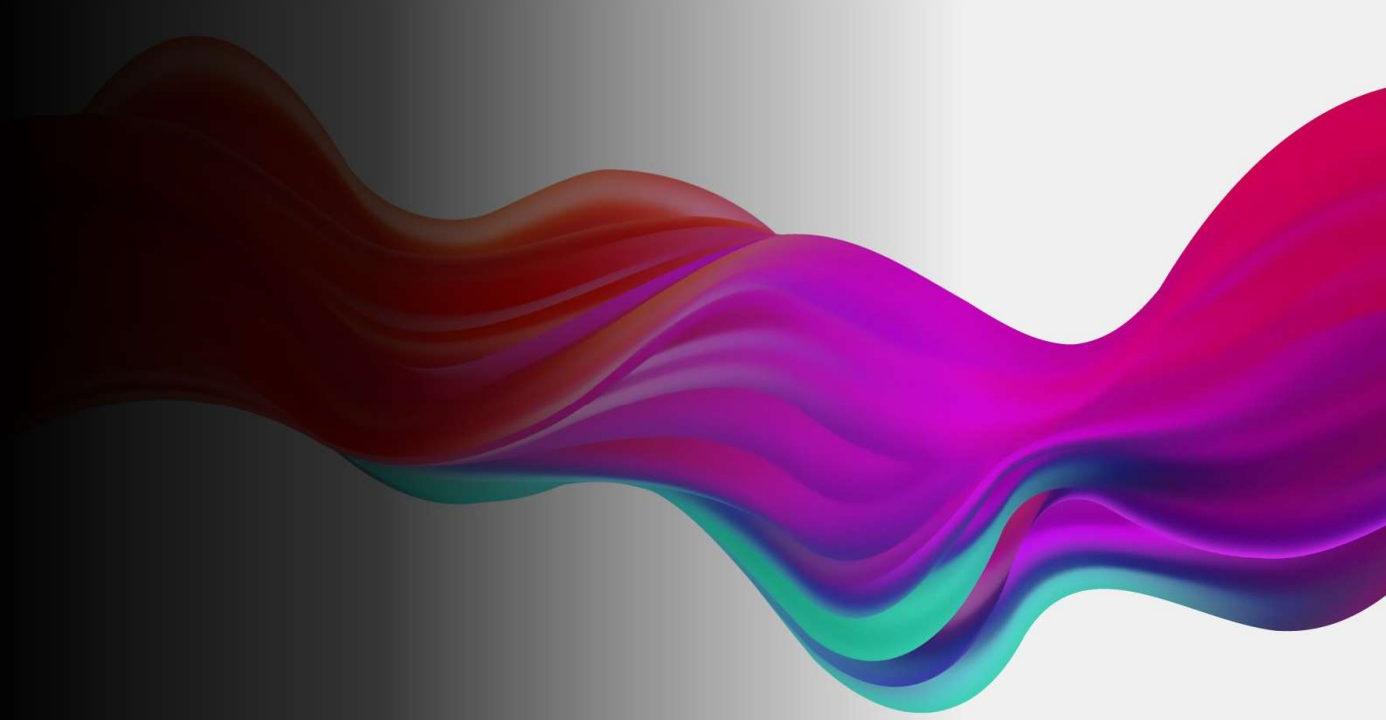
Traditional Model

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

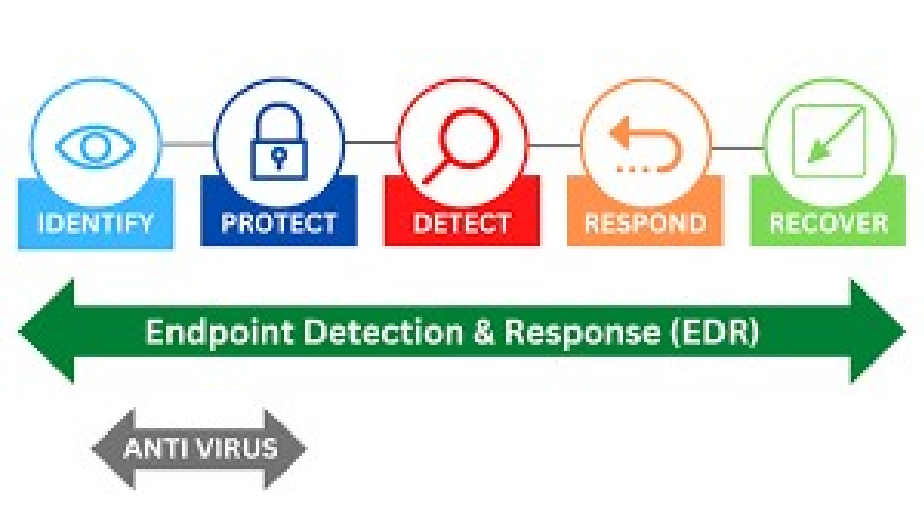


Encryption and Data Protection:

- 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)

Door

Indoor motion sensor $50

Indoor Camera $500

Window bars

Outdoor Camera $1,000

Cloud based storage for video recording $500 per year

Provide labels here for any symbols you use!

1

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)

Door

Indoor motion sensor $50

Indoor Camera $500

Window bars

Outdoor Camera $1,000

Cloud based storage for video recording $500 per year

Provide labels here for any symbols you use!

1

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

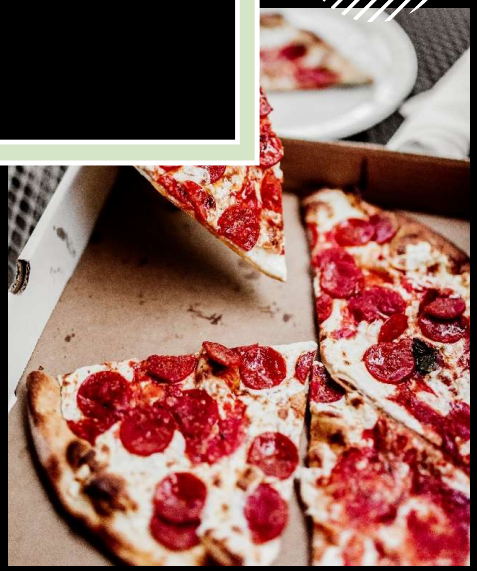
Go to a Restaurant

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?

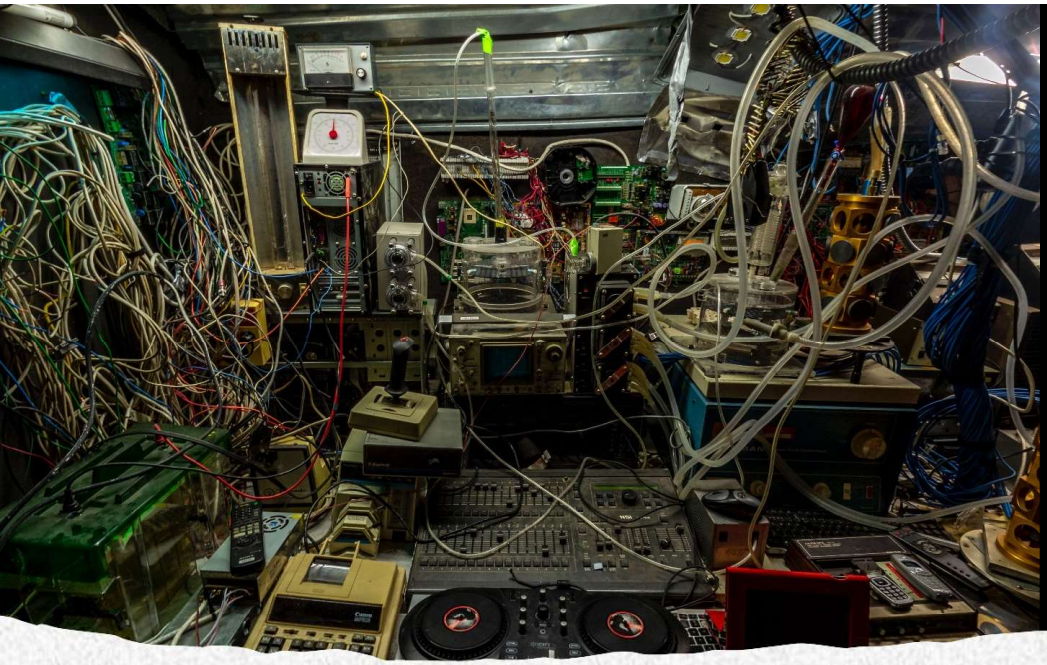
Pizza as a Service 2.0

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

Configuration
Functions
Scaling
Runtime
OS
Visualization
Hardware

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)

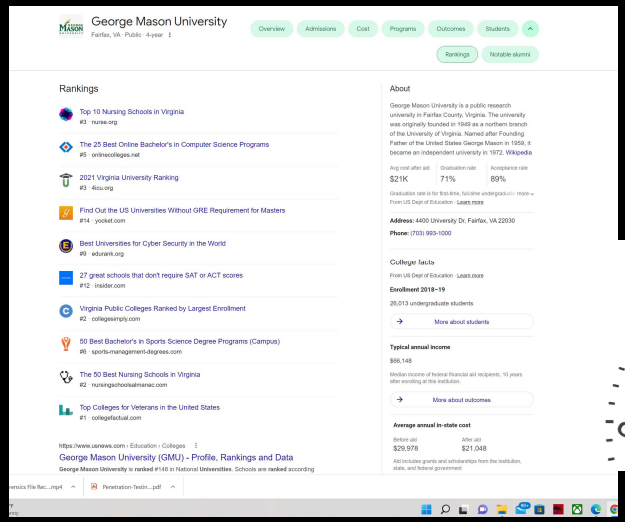
Trust

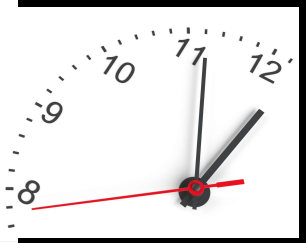
What makes us trust someone to do what we have hired them to do and how do we do this in a systematic fashion?

Great Service

Excellent

Five Stars

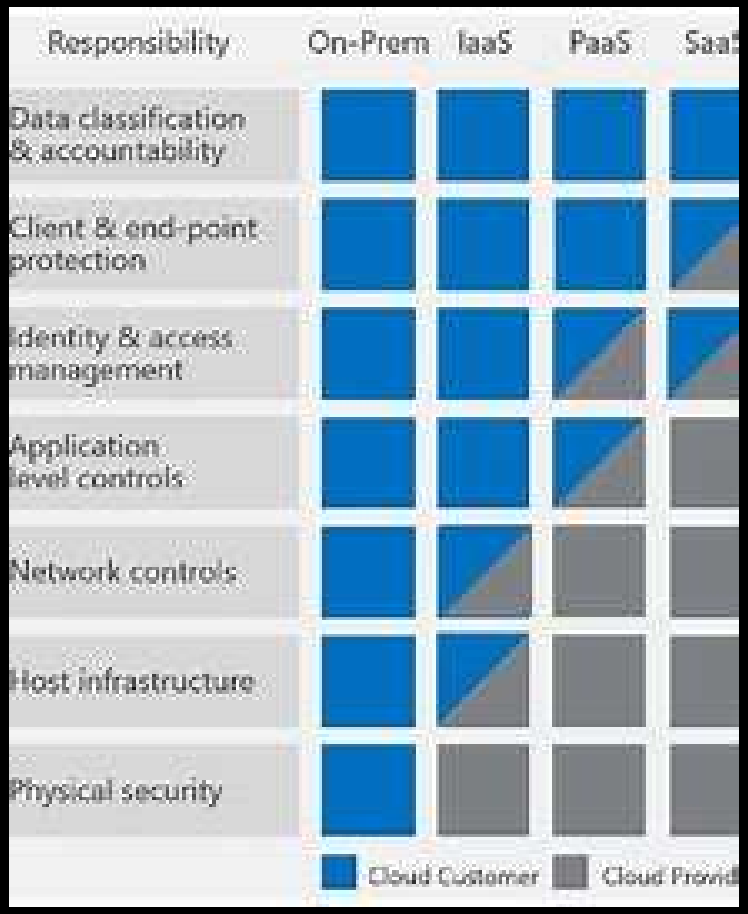




Cloud Shared Responsibility

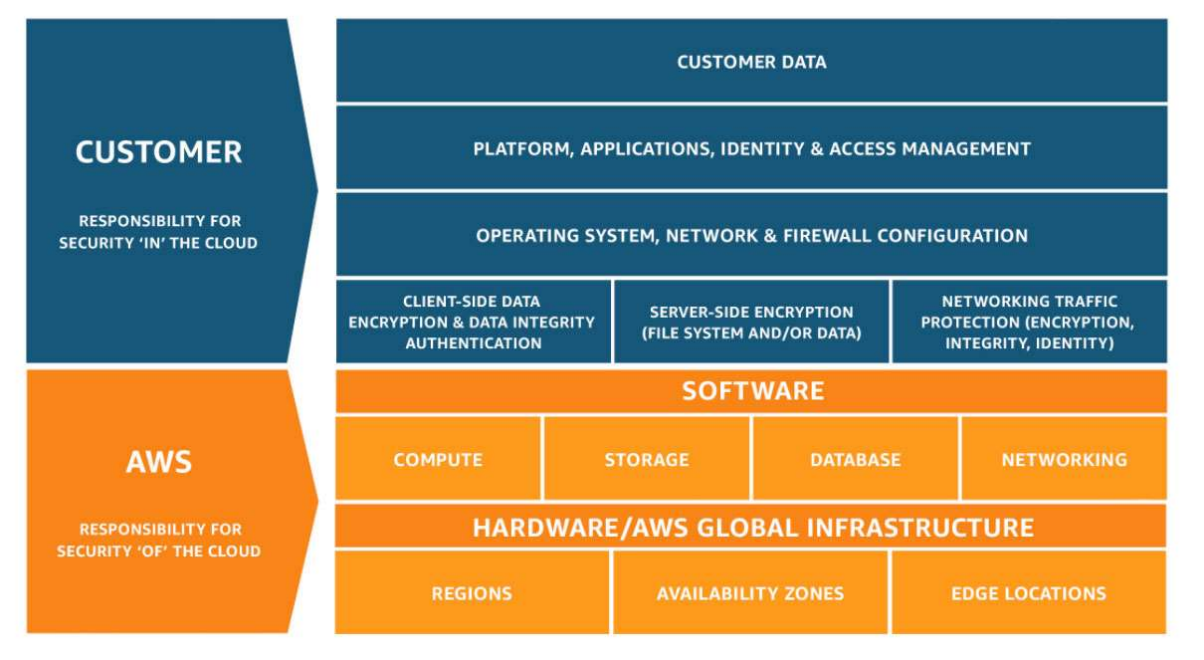
Security and Compliance is a shared responsibility between the CSP and the customer.

The responsibility changes according to the deployment model



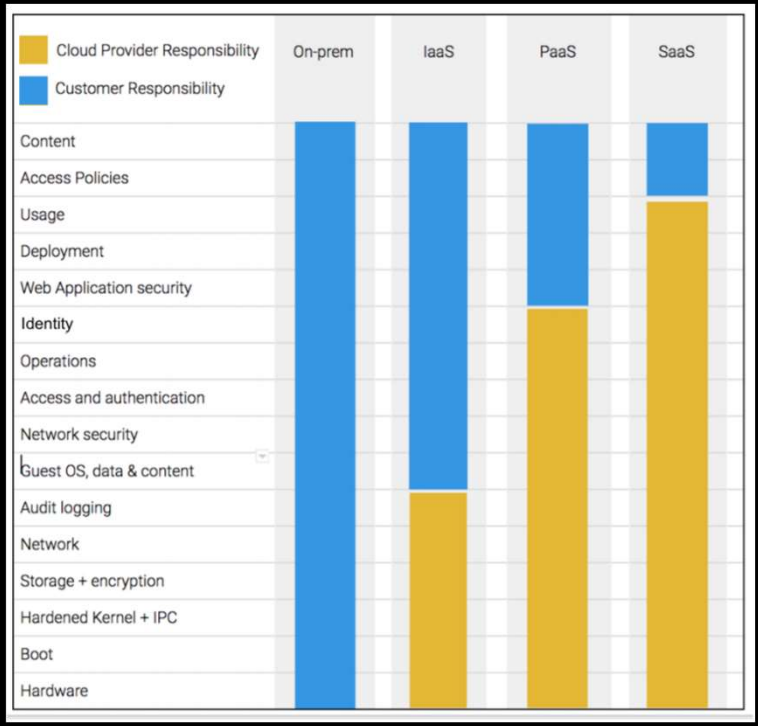
[Diagram from Shared Responsibility for Security Privacy and Compliance in Microsoft Azure]

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

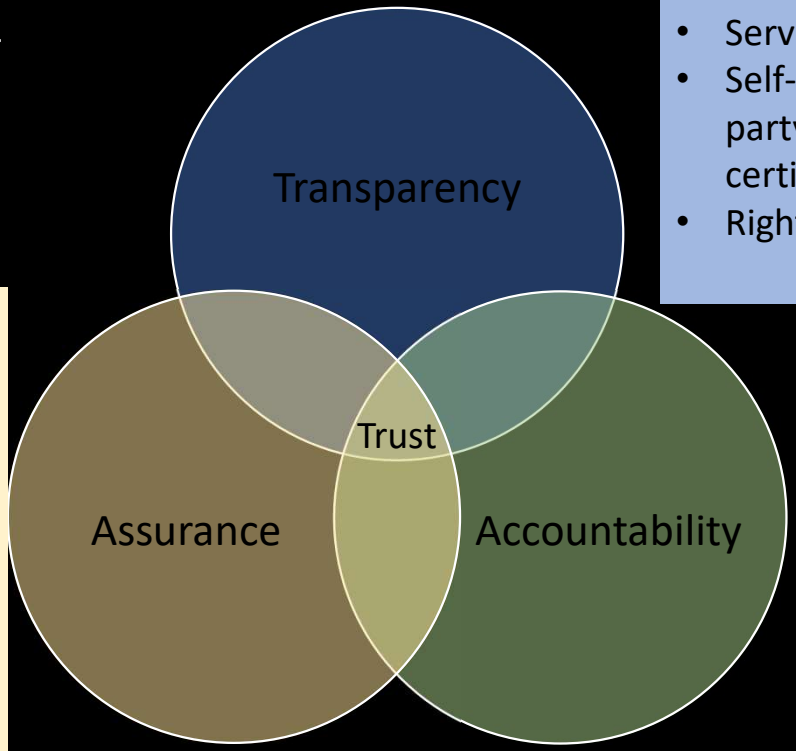
When does a team win?

- 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

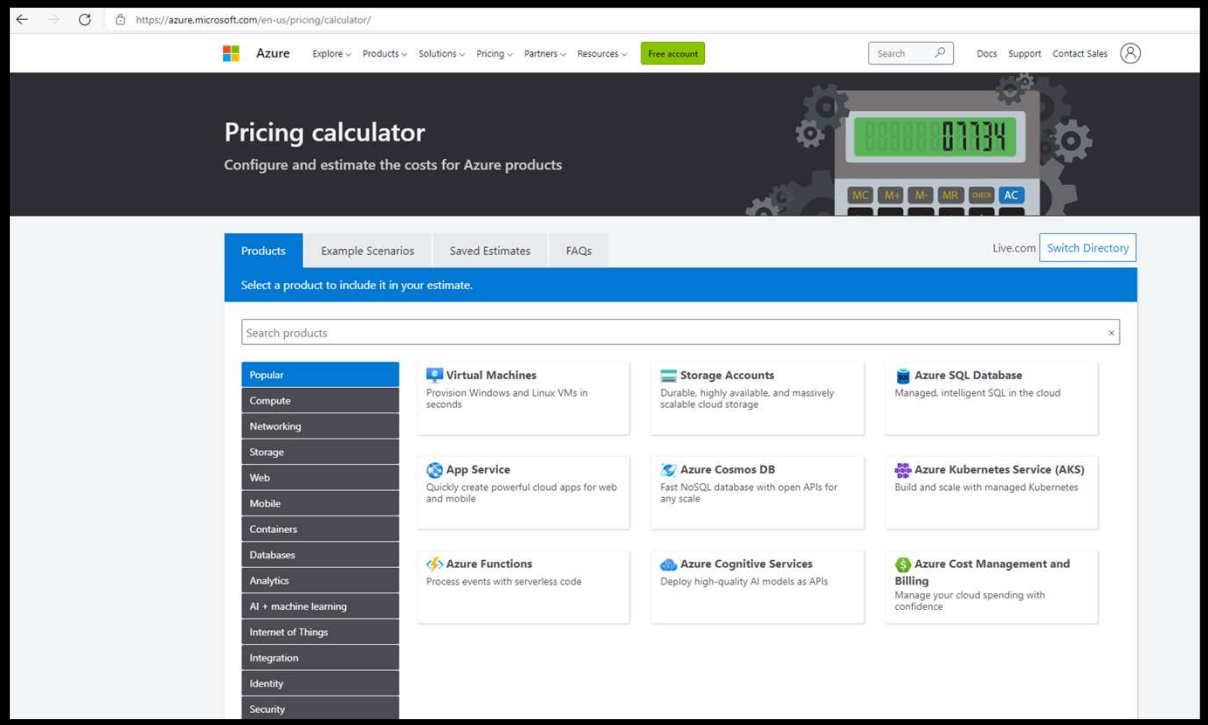
What are the benefits of Cloud?

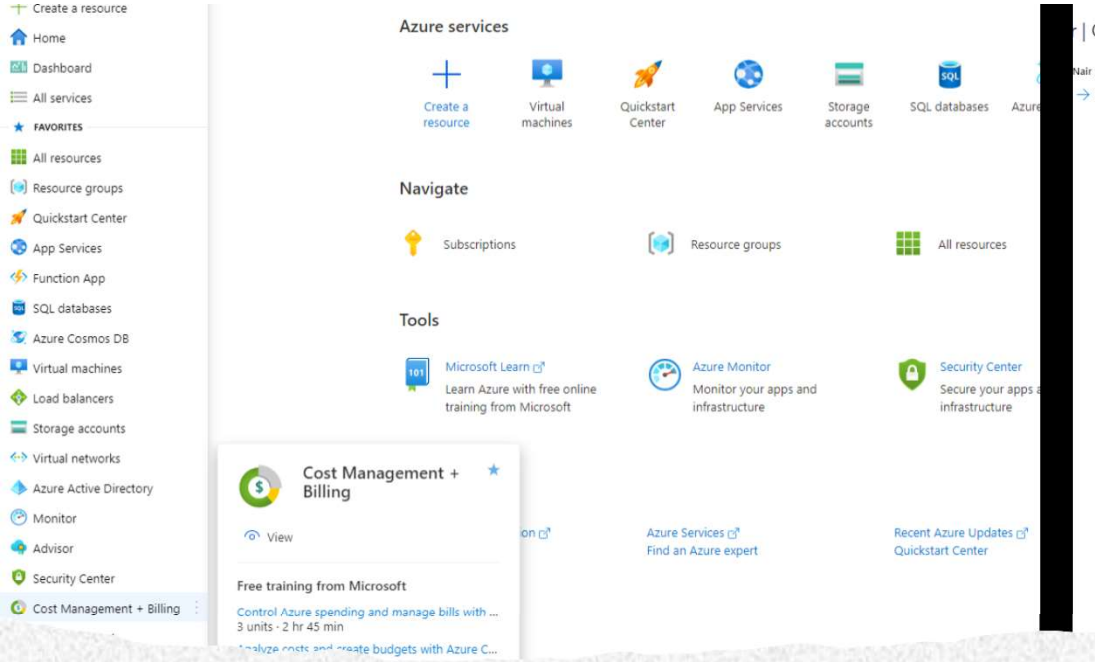
- Cost Saving
- Availability/Reliability
- Flexibility/Elasticity/Scalability
- Security
- Agility
- Optimized Resource Utilization
- Access to skills and capabilities
- Performance

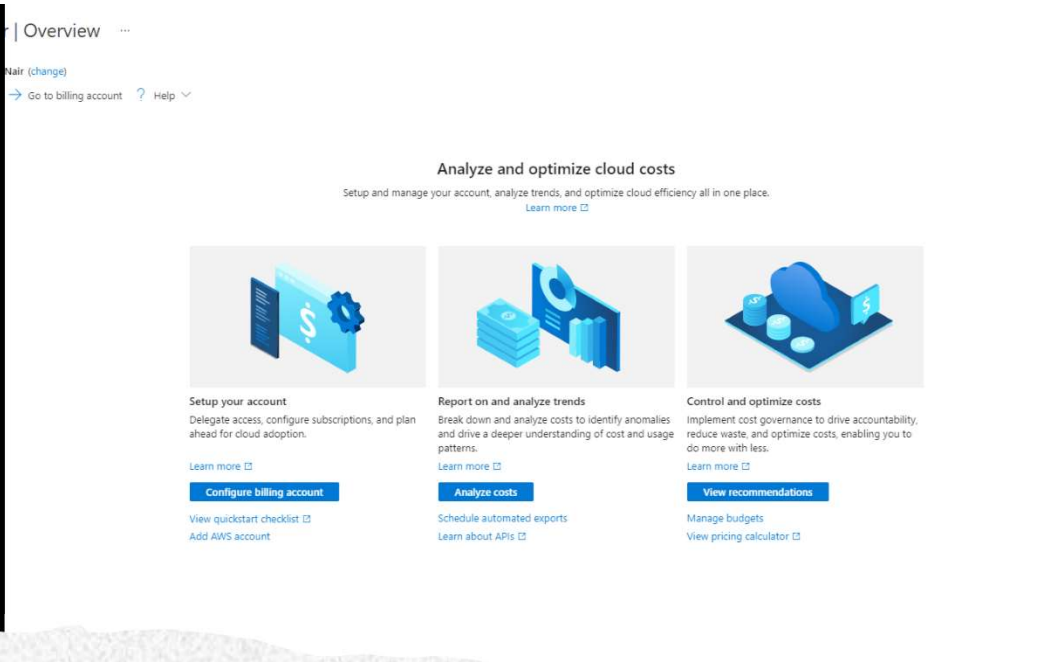
Cloud definition from NIST SP 800-145, The NIST Definition of Cloud Computing

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

Image copyright Amazon

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

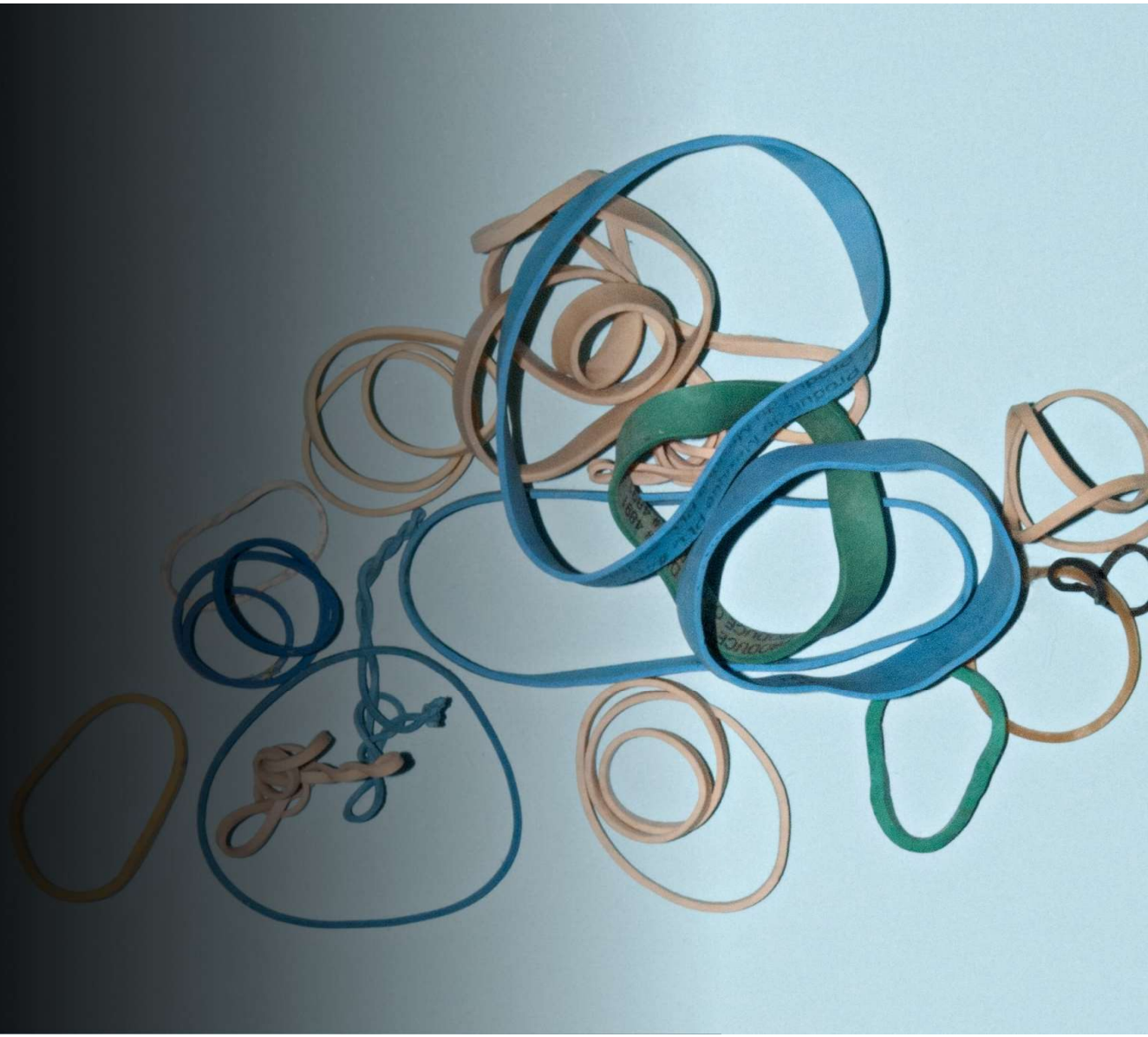
Image copyright Google

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?

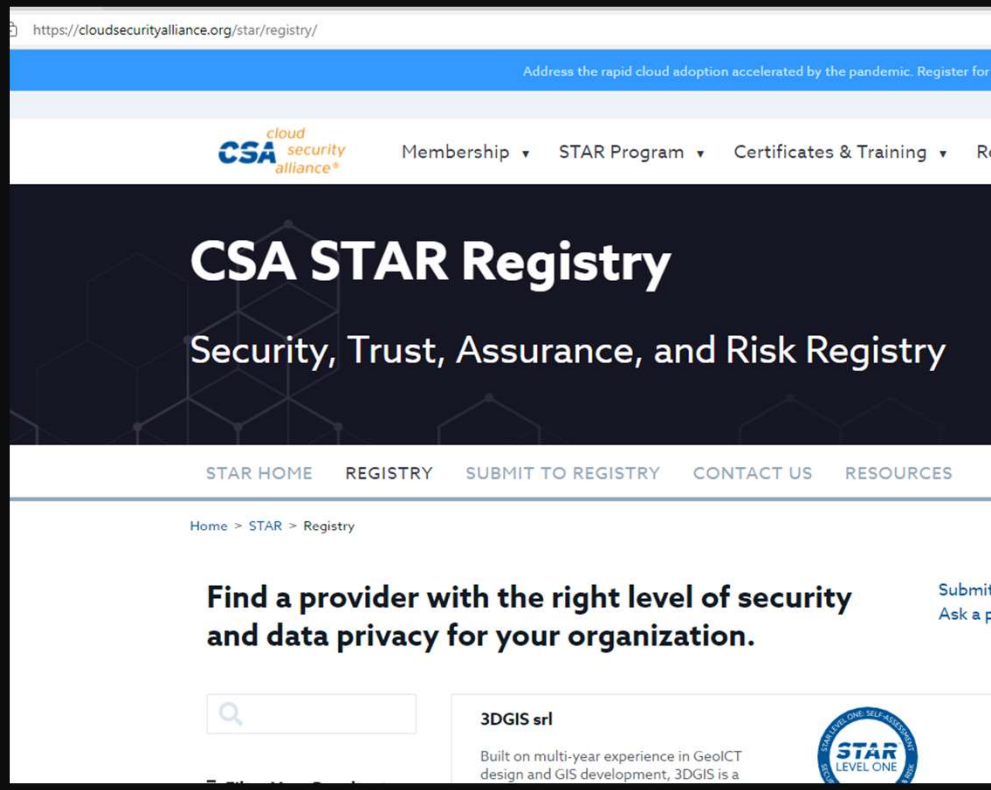
- Cost Saving
- Availability/Reliability
- Flexibility/Elasticity/Scalability
- Security
- Agility
- Increased collaboration
- Optimized Resource Utilization
- Access to skills and capabilities
- Performance

- 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



Demo: CSA STAR

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

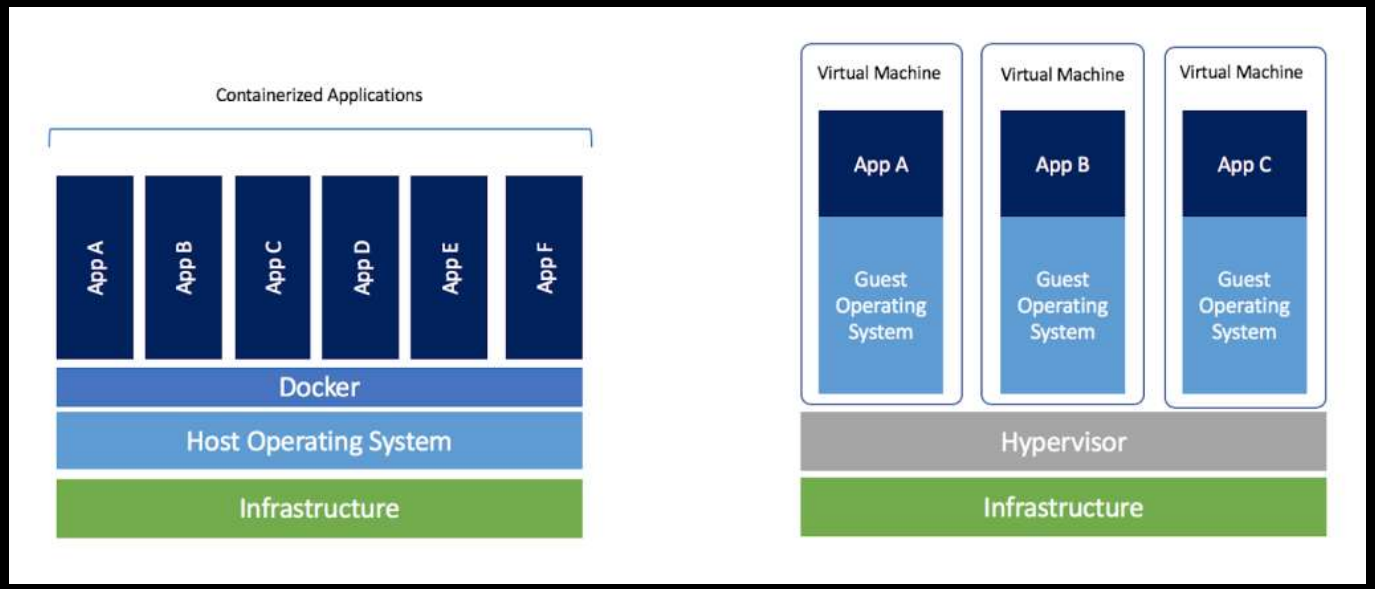
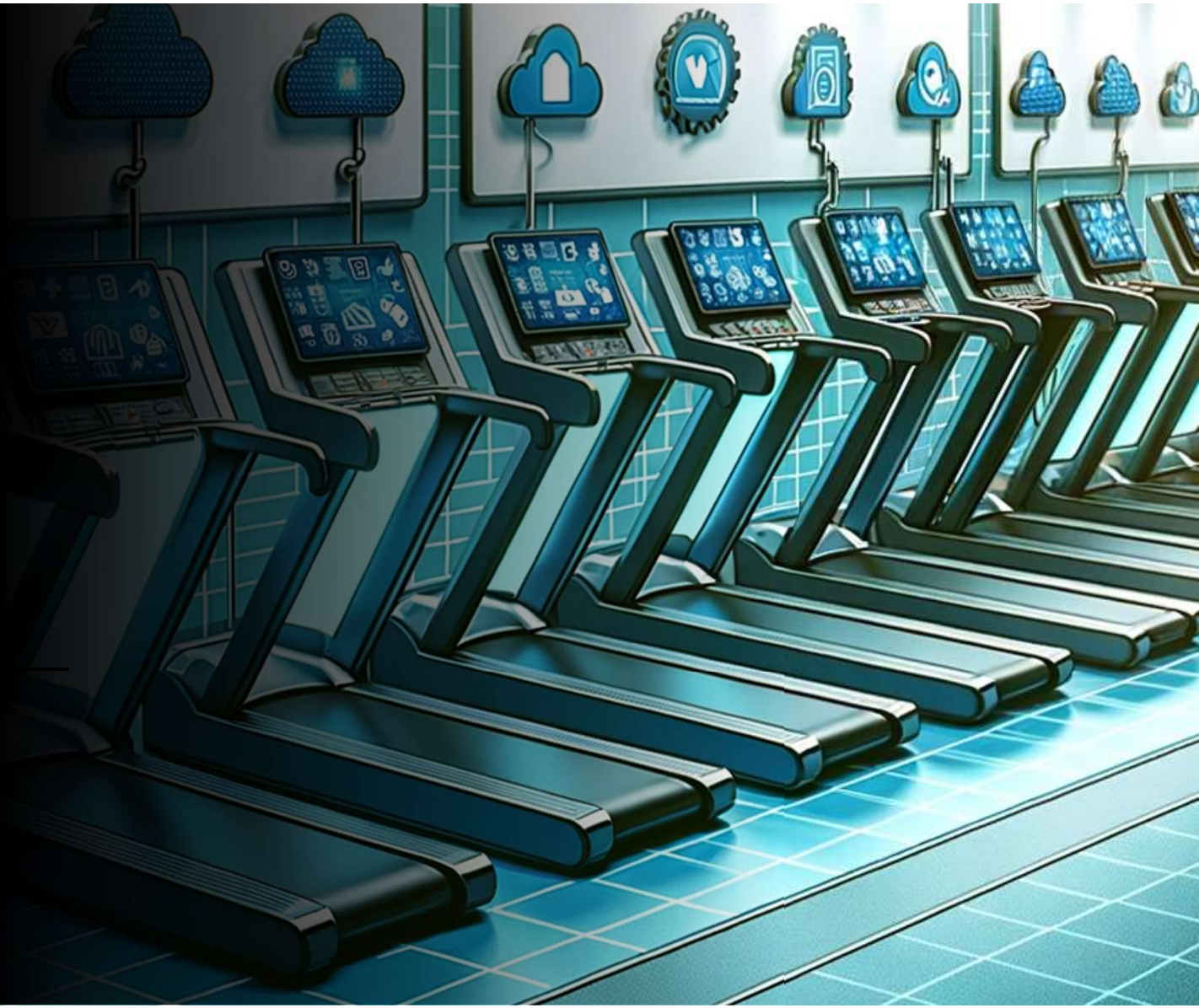


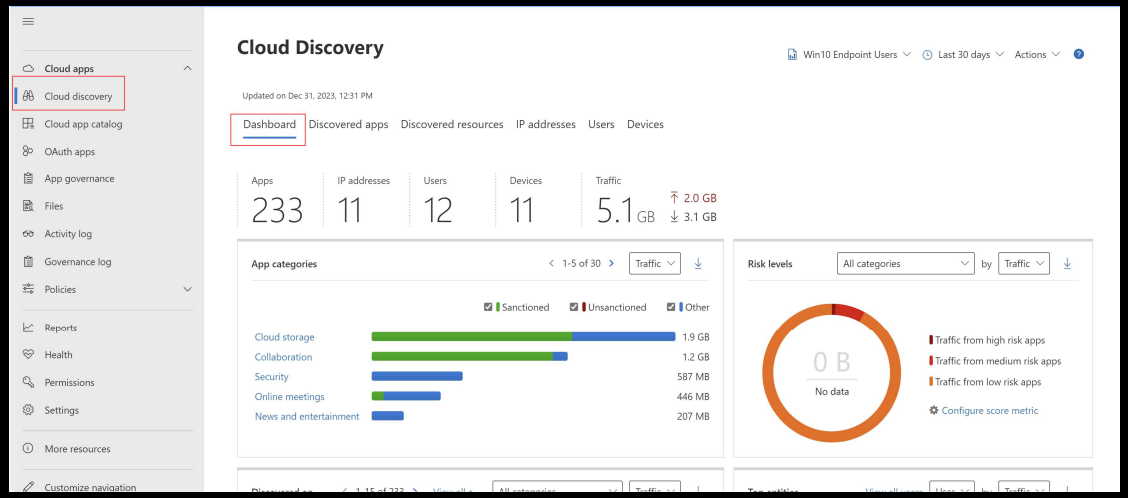
Image from https://www.docker.com/blog/containers-replacing-virtual-machines/

Serverless

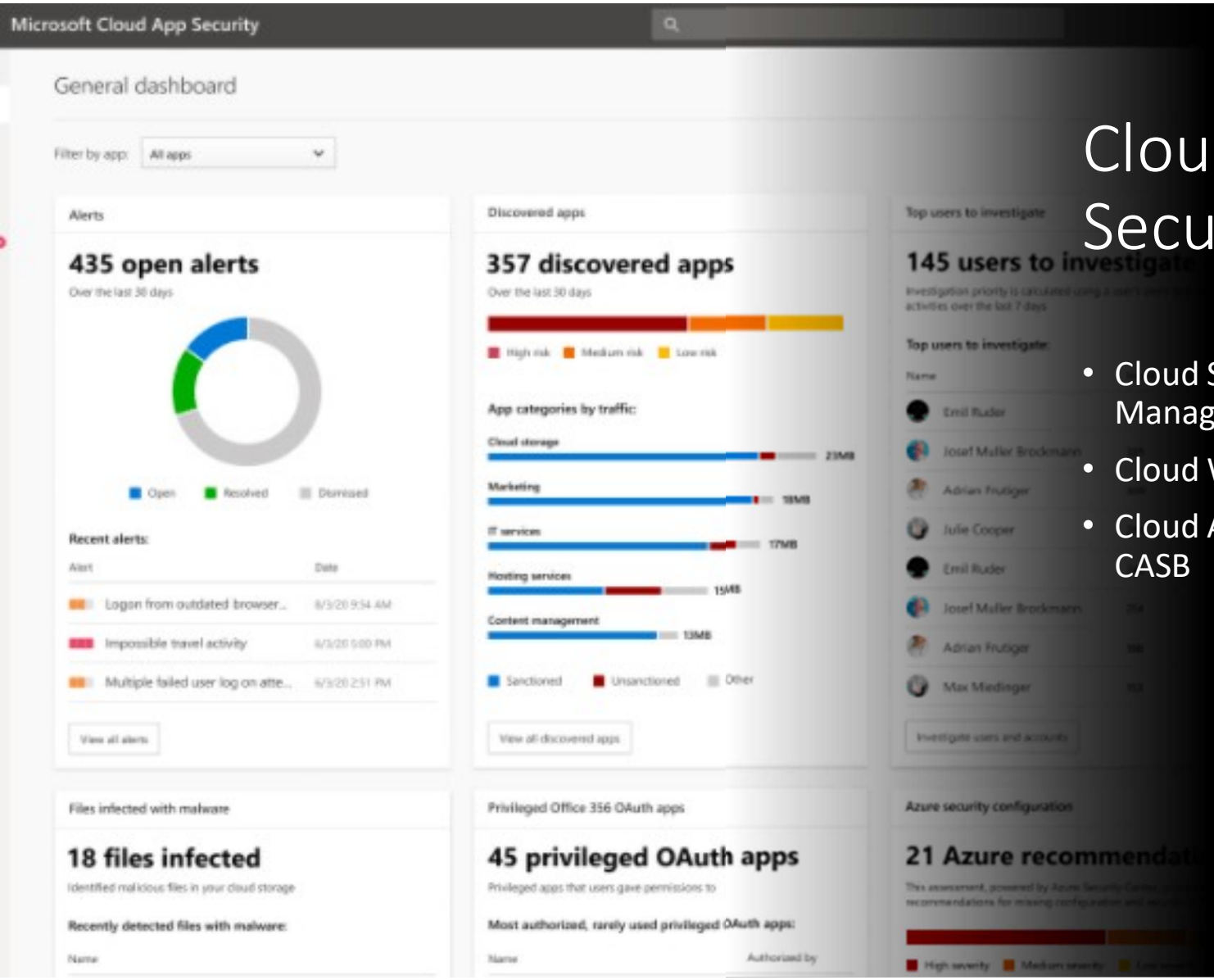


How do I know what I have in the cloud?

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



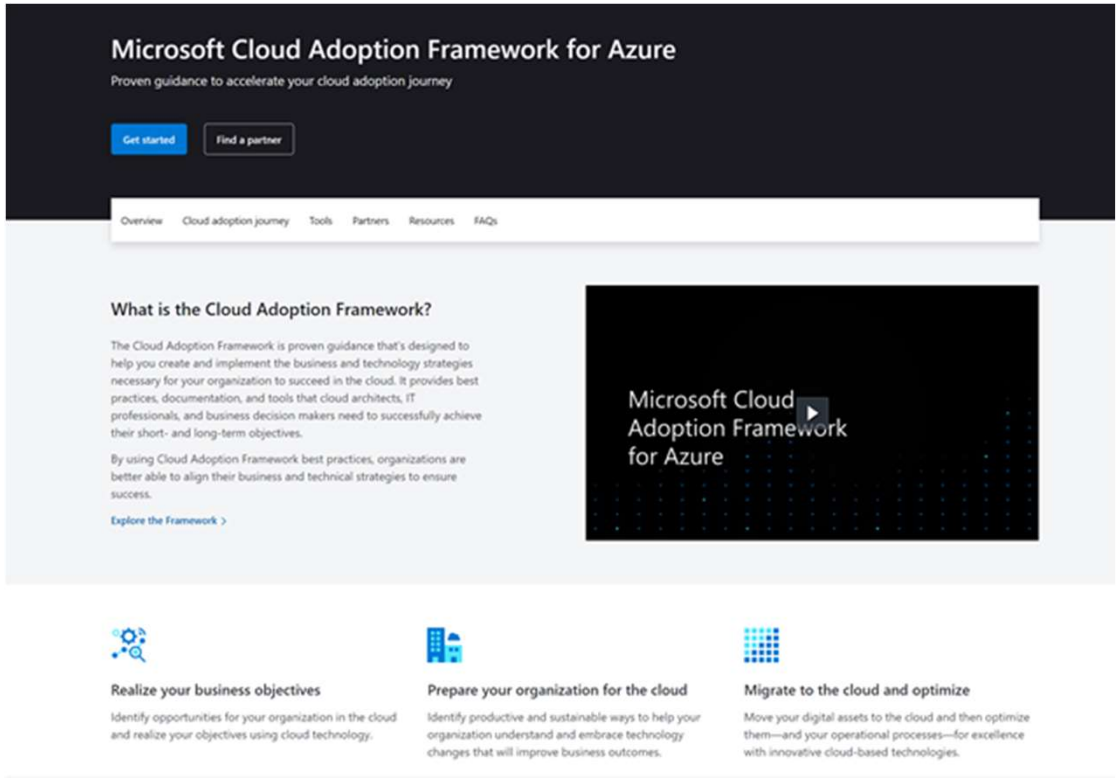
You can't protect what you can't see



Cloud Specific Security Tools

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

How do you securely use the cloud?



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

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

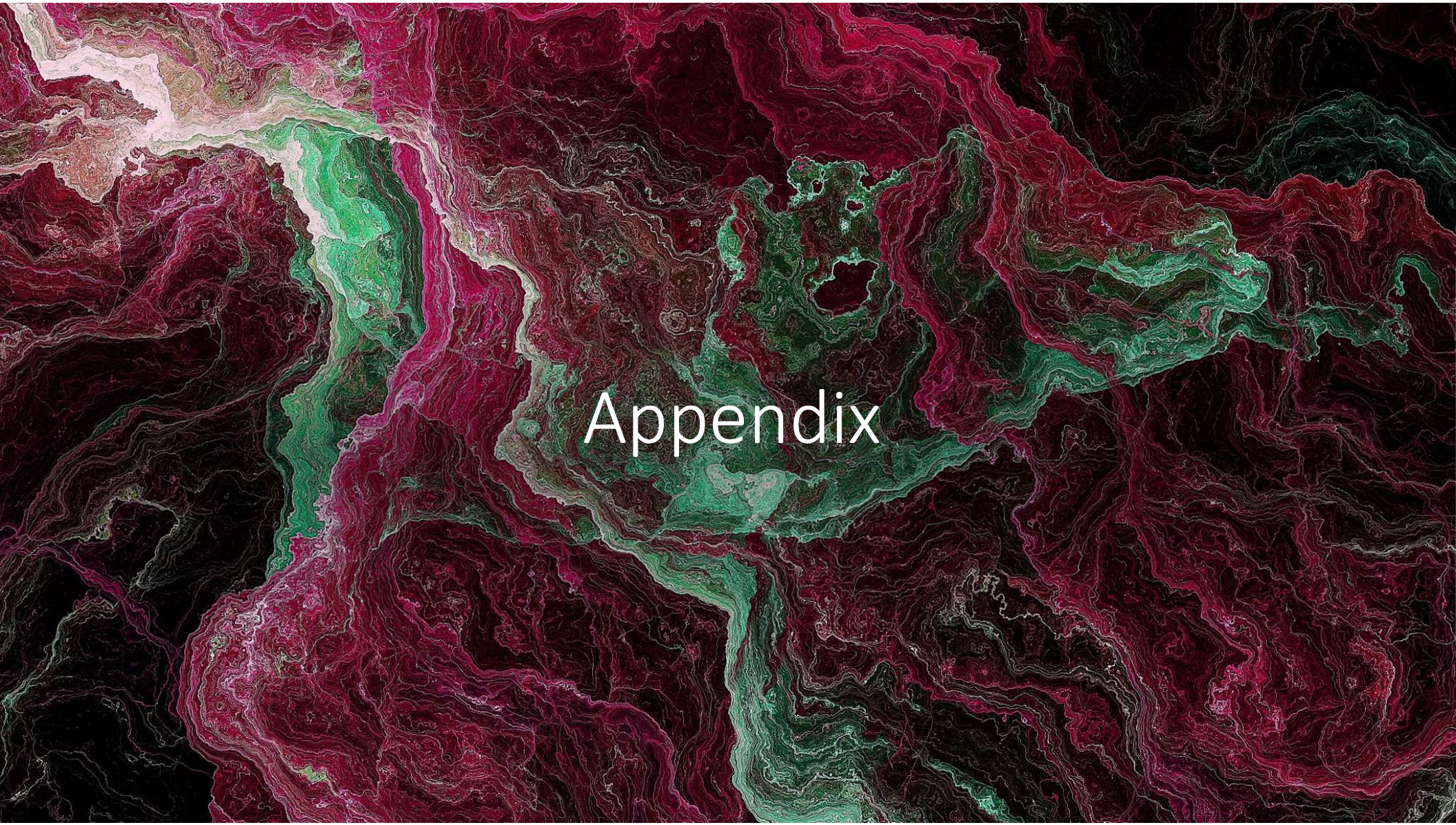
Learning more about cybersecurity and Cloud

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

Thank you

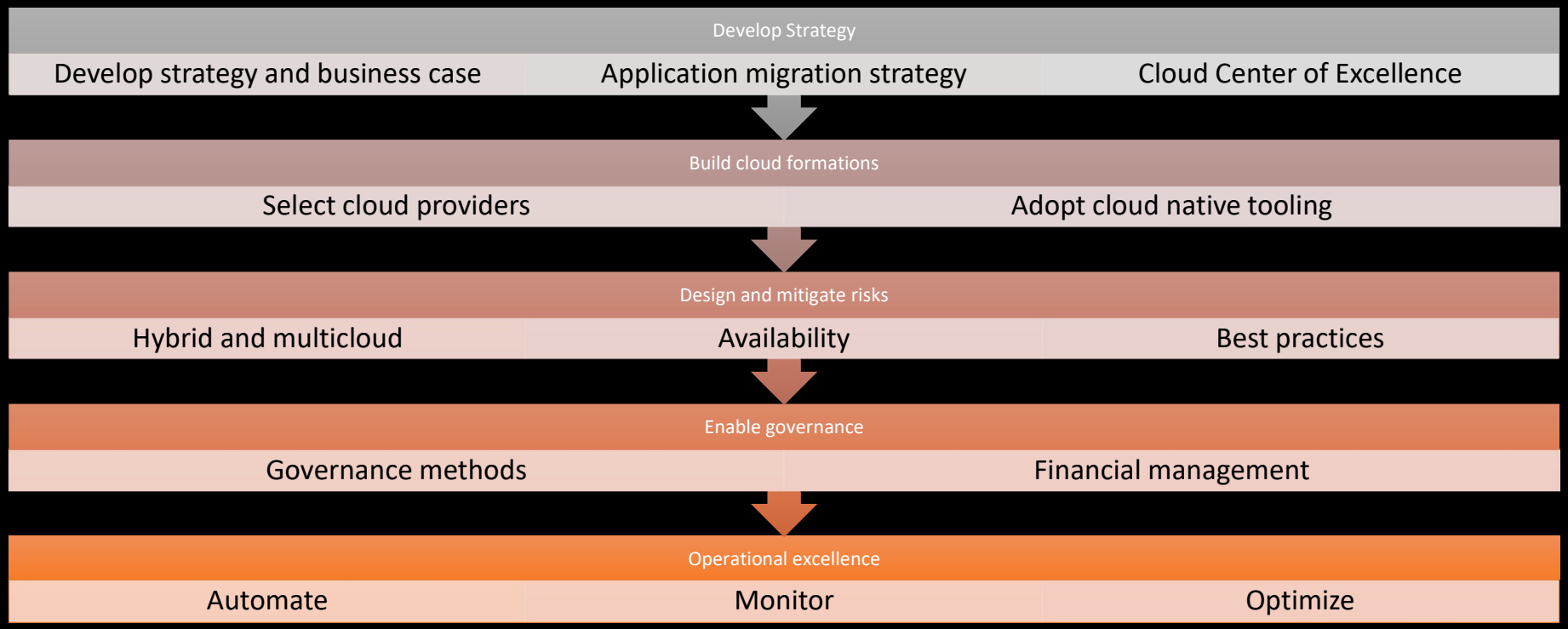
- Any questions???
- Contact nairsushi@gmail.com
- Follow me on LinkedIn https://www.linkedin.com/in/sushilanair/
- Twitter @sushila_nair

Community builds our skills and network



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?

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

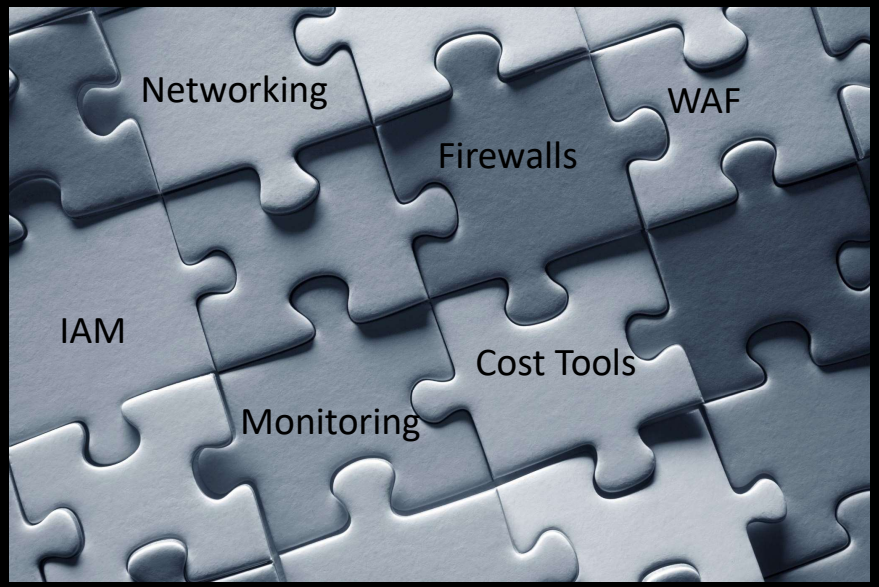
- Cloud Native
- CSP Native
- Born in the cloud

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

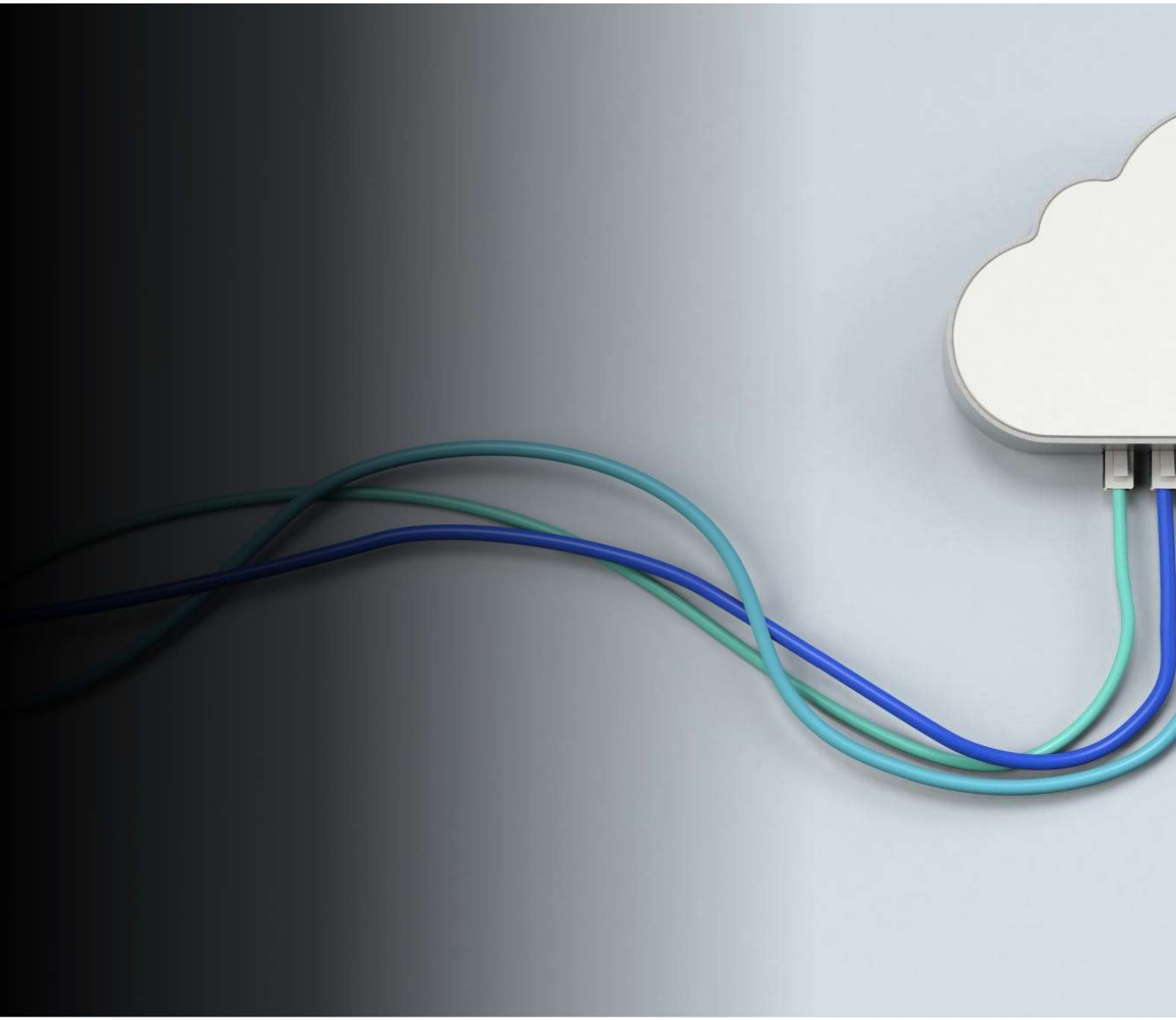


3. Design and Mitigate Risk

- 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.

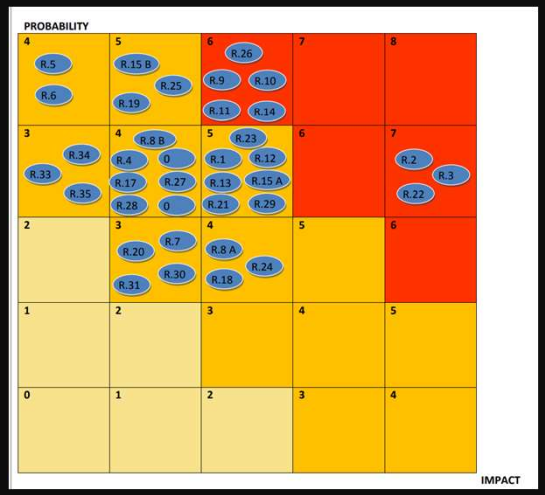
- Google Cloud Platform: Google Deployment Manager allows the use of flexible template and configuration files leveraging Yaml - or Python and Jinja2 templates to configure deployments.

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

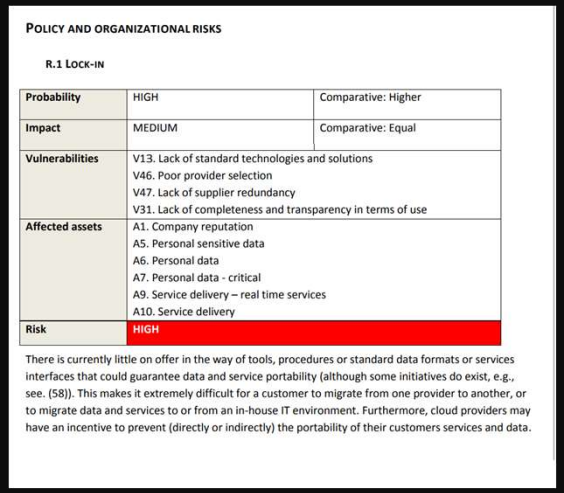
- The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact.
- The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.



Low risk: 0-2

Medium Risk: 3-5

High Risk: 6-8



POLICY AND ORGANIZATIONAL RISKS

R.1 LOCK-IN

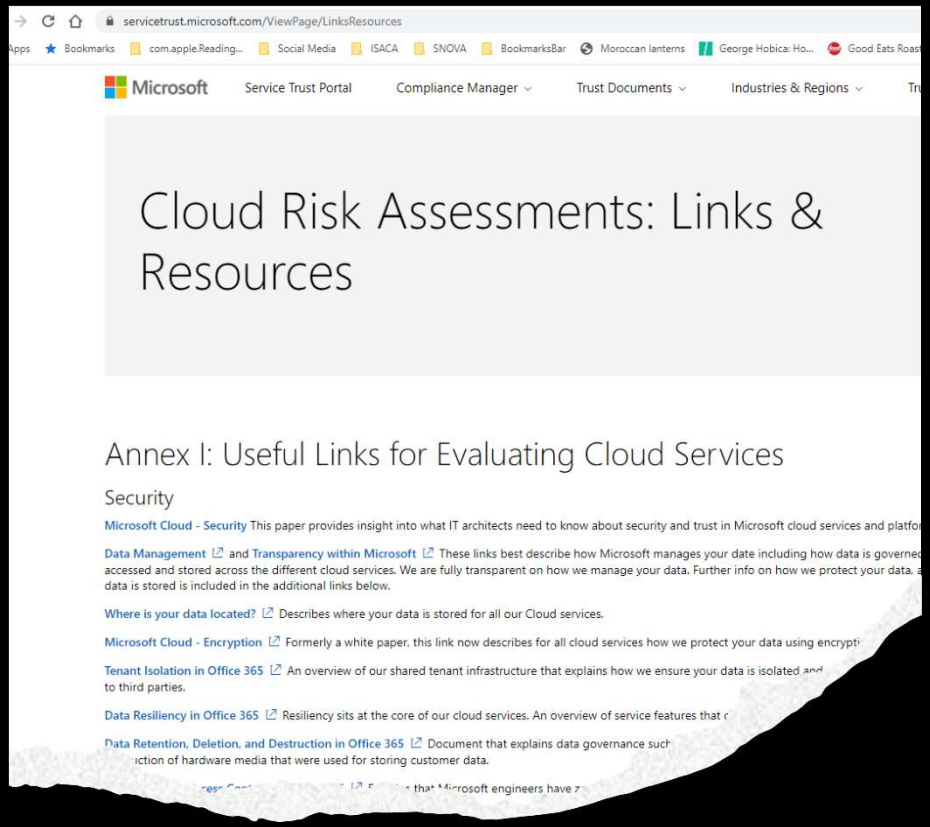
Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

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.

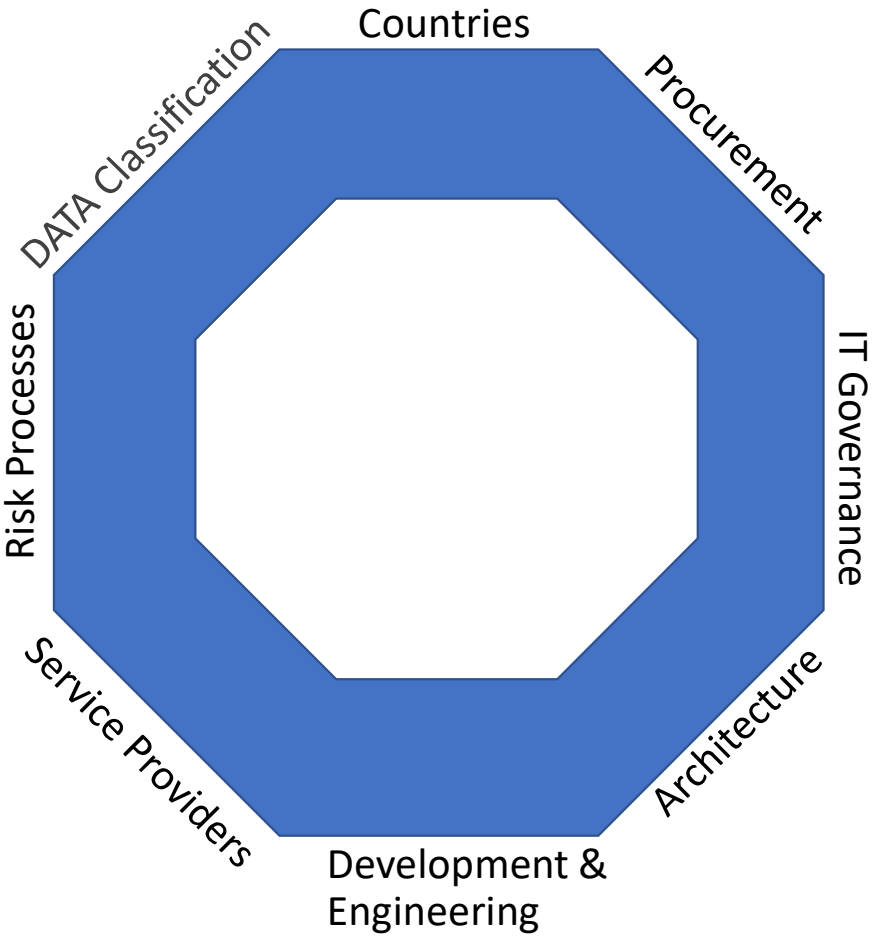
https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

Cloud Risk resources

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



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

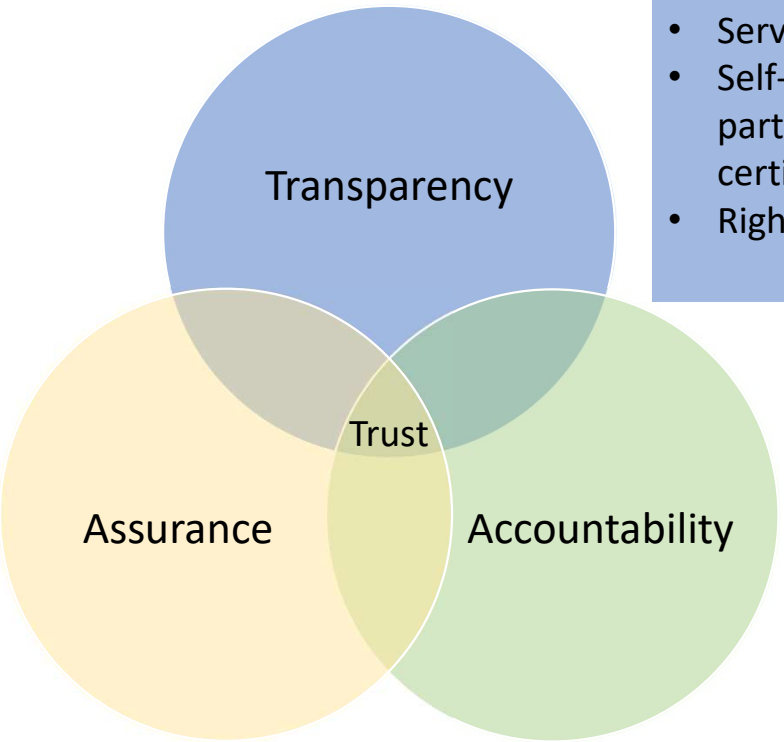
Discussion

- 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.

- 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

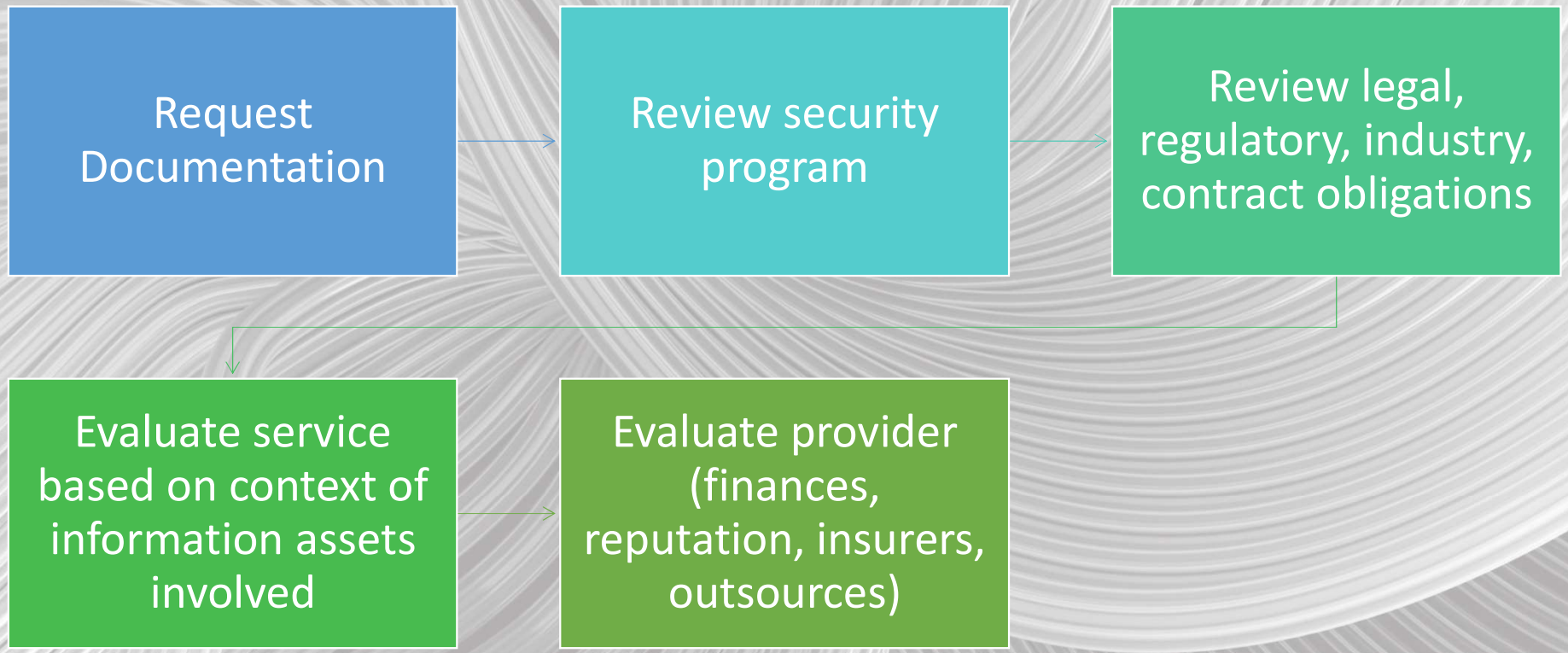
Responsiveness
Responsibility
Remediability

Defining Trust

- The CSA defines trust as a function of assurance, transparency and accountability

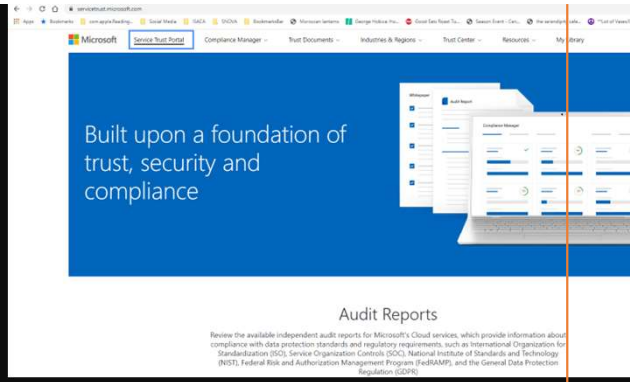
- The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings

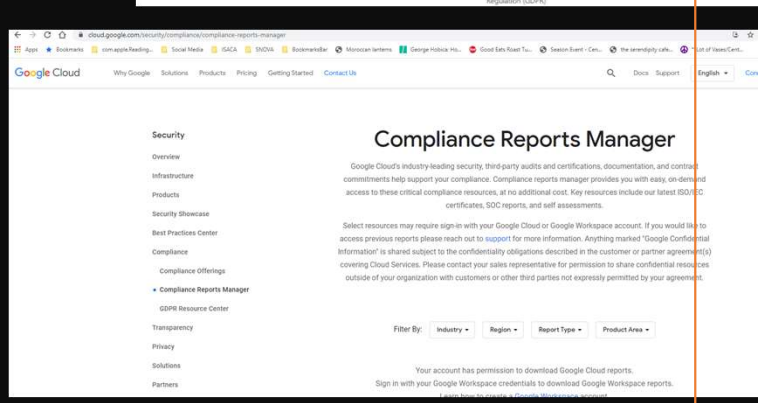
Reminder – This documentation is used for cloud provider selection and ongoing assessment

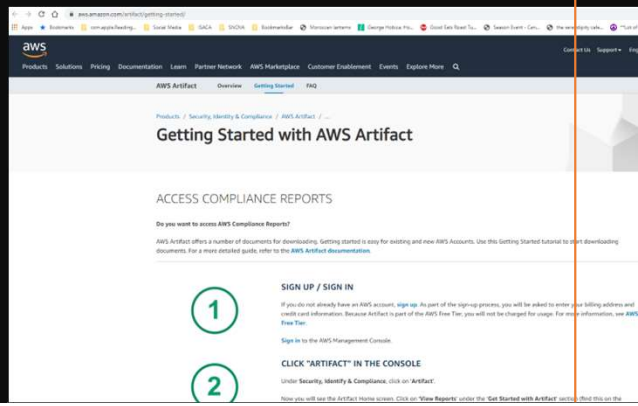


Accessing CSP audit reports

- 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)
- 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