



NEW YORK **M**ETRO **J**OINT
CYBER **S**ECURITY **C**ONFERENCE

September 26, 2024

<https://InfoSecurity.NYC>



Adnan Rafique

**Securing the Cloud:
Strategies for Comprehensive Cloud
Security Management**

Cloud Security Management

Key Take Aways



Gain insight into the unique challenges of securing data and systems in the cloud.

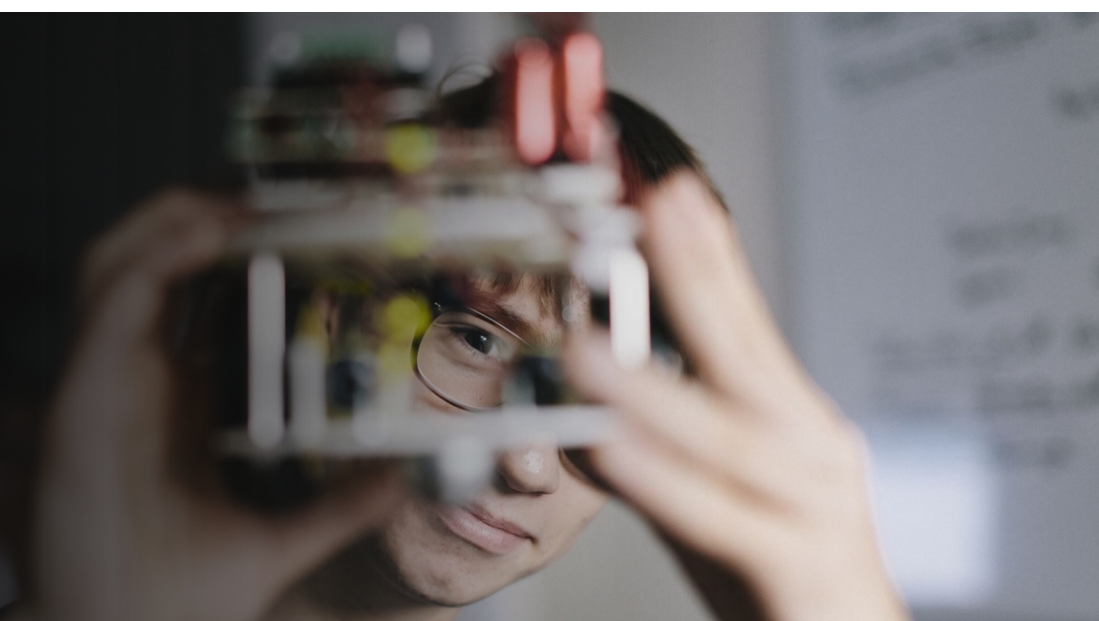
Practical strategies to reduce risks and keep their organization's information safe in the cloud.

Empower cybersecurity professionals, giving them confidence to tackle cloud security complexities effectively.

DISCLAIMER

The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect the official policy or position of my current employer. This educational session is intended for informational purposes only and is based on personal experience and research.

Who am I?



```
irobot@Adnan-M3 ~ % whoami
irobot
irobot@Adnan-M3 ~ % id -F
Adnan Rafique
irobot@Adnan-M3 ~ % █
```

ADNAN RAFIQ-UE CISM

Adnan Rafique | CISM

2x Microsoft MVP M365

<https://www.linkedin.com/in/arafique1/>

www.iMentorCloud.com

[Youtube.com/@iMentorCloud](https://www.youtube.com/@iMentorCloud) – 10K

CSA CCSK 5.0 - Contributor



Adnan Rafique
CISM | Information Security Leader | Speaker



Gadgets | Travel | Photography | Foodie

ECHOES OF THE PAST

**“Those who cannot remember
the past are condemned
to repeat it.” — George Santayana**

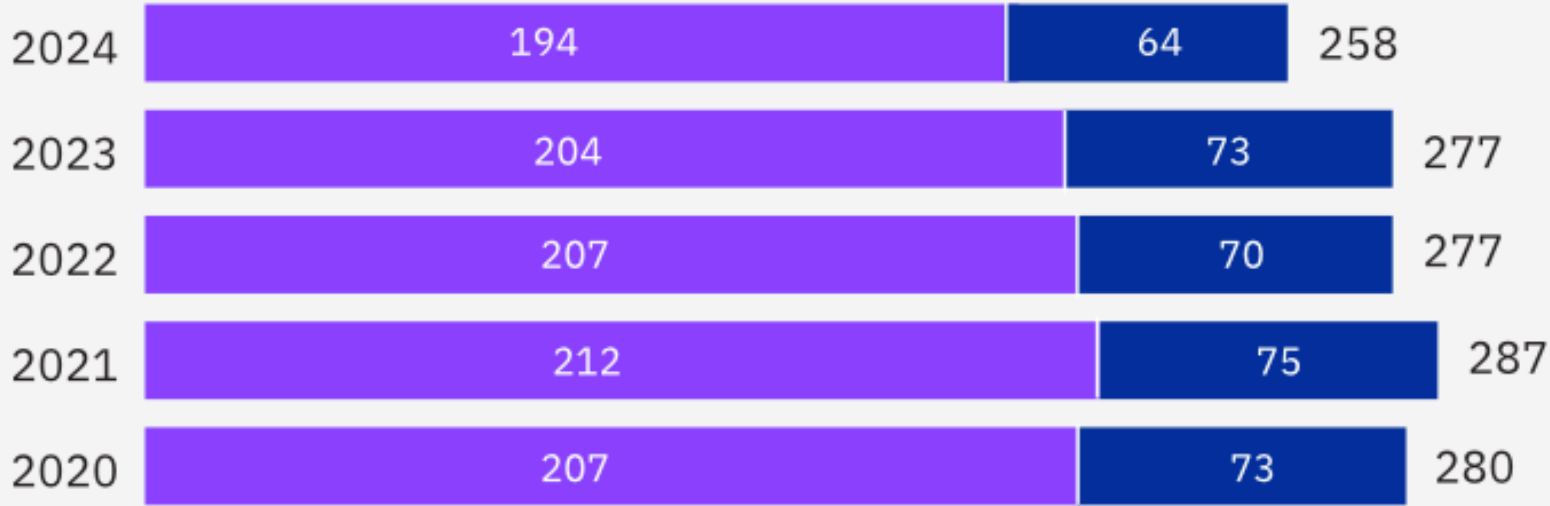
This famous quote suggests that understanding past experiences is crucial to avoid repeating the same mistakes, implying that learning from history helps shape a better future.

292

Days to identify and contain breaches involving stolen credentials

Breaches involving stolen or compromised credentials took the longest to identify and contain (292 days) of any attack vector. Similar attacks that involved taking advantage of employees and employee access also took a long time to resolve. For example, phishing attacks lasted an average of 261 days, while social engineering attacks took an average of 257 days.

Time to identify and contain a data breach



Source : IBM - Data Breach Report 2024

Top 5 categories in response time

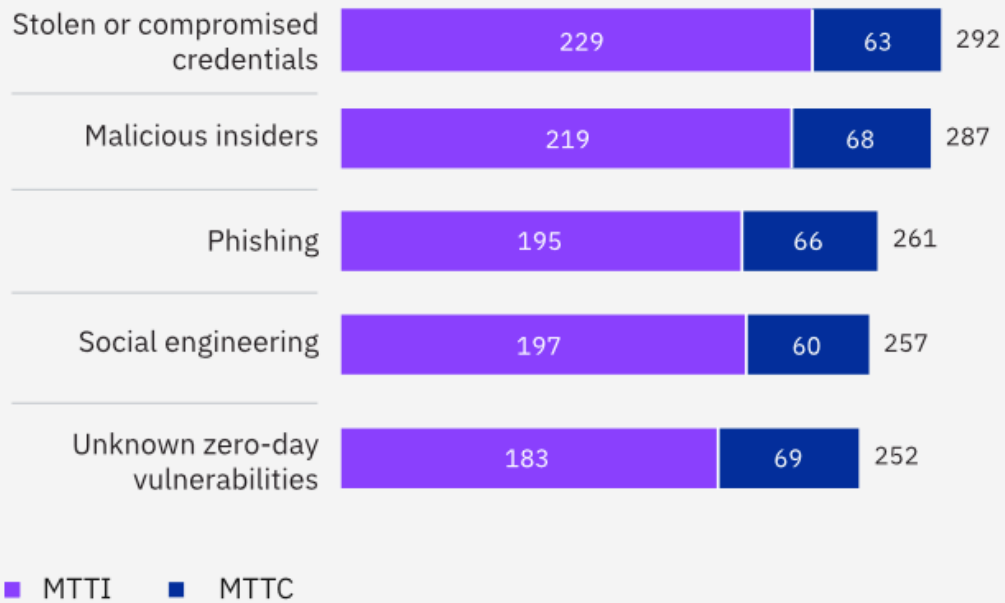
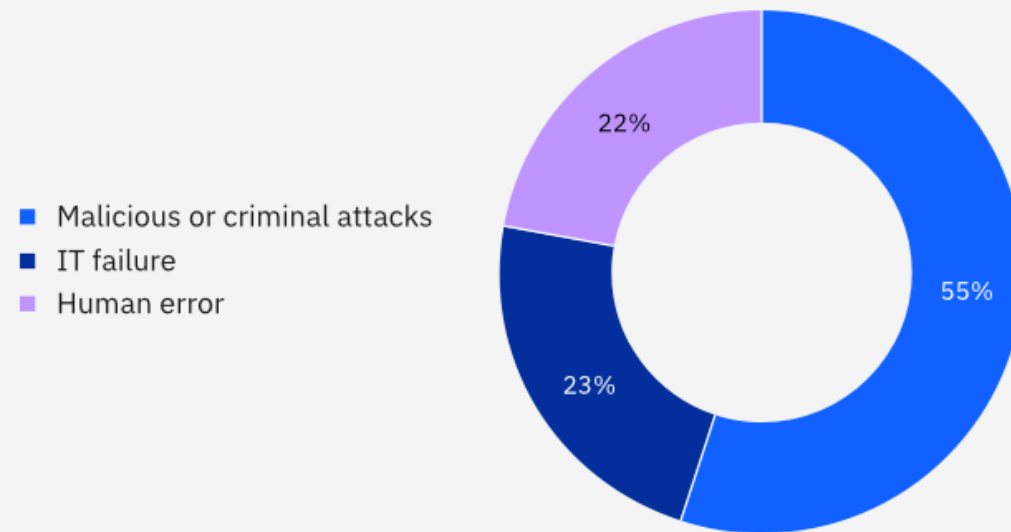


Figure 8. Measured in days

Source : IBM - Data Breach Report 2024

Root cause of the data breach between 3 categories



Source : IBM - Data Breach Report 2024

Most breaches involved customer PII

The most common type of data stolen or compromised was customer PII, at 46%. PII can include tax ID numbers, emails and home addresses, and can be used in identity theft and credit card fraud. The global average for all stolen record types rose to a high of USD 169, with employee PII the costliest. See Figures 6A and 6B.

Left it intentionally

Cool stuff



National Public Data Breach

- Full names
- Dates of birth
- 420 million distinct addresses
- 272 million distinct US Social Security Numbers (SSNs)
- Over 161 million distinct phone numbers



10 worst AWS S3 Breaches

Notable Data Breaches:

Booz Allen Hamilton:

Exposed battlefield imagery and admin credentials in May 2017 due to insecure S3 settings.

U.S. Voter Records: Deep Root Analytics leaked personal data of 198 million voters in June 2017.

Dow Jones & Co: Personal info of 2.2 million people exposed in July 2017 due to improper S3 permissions.

WWE: Leaked personal details of over 3 million fans in July 2017.

Verizon Wireless: Exposed 6 million customer records and sensitive corporate data in two incidents (July and September 2017).

Time Warner Cable: Leaked data about 4 million customers and proprietary code in September 2017.

Pentagon: Multiple leaks in September and November 2017, including sensitive intelligence data and personal resumes.

Accenture: Exposed master access keys and critical infrastructure data in October 2017.

National Credit Federation: Leaked 111GB of financial data about 47,000 people in December 2017.

Alteryx: Exposed personal information of 123 million American households in December 2017.

Apply this

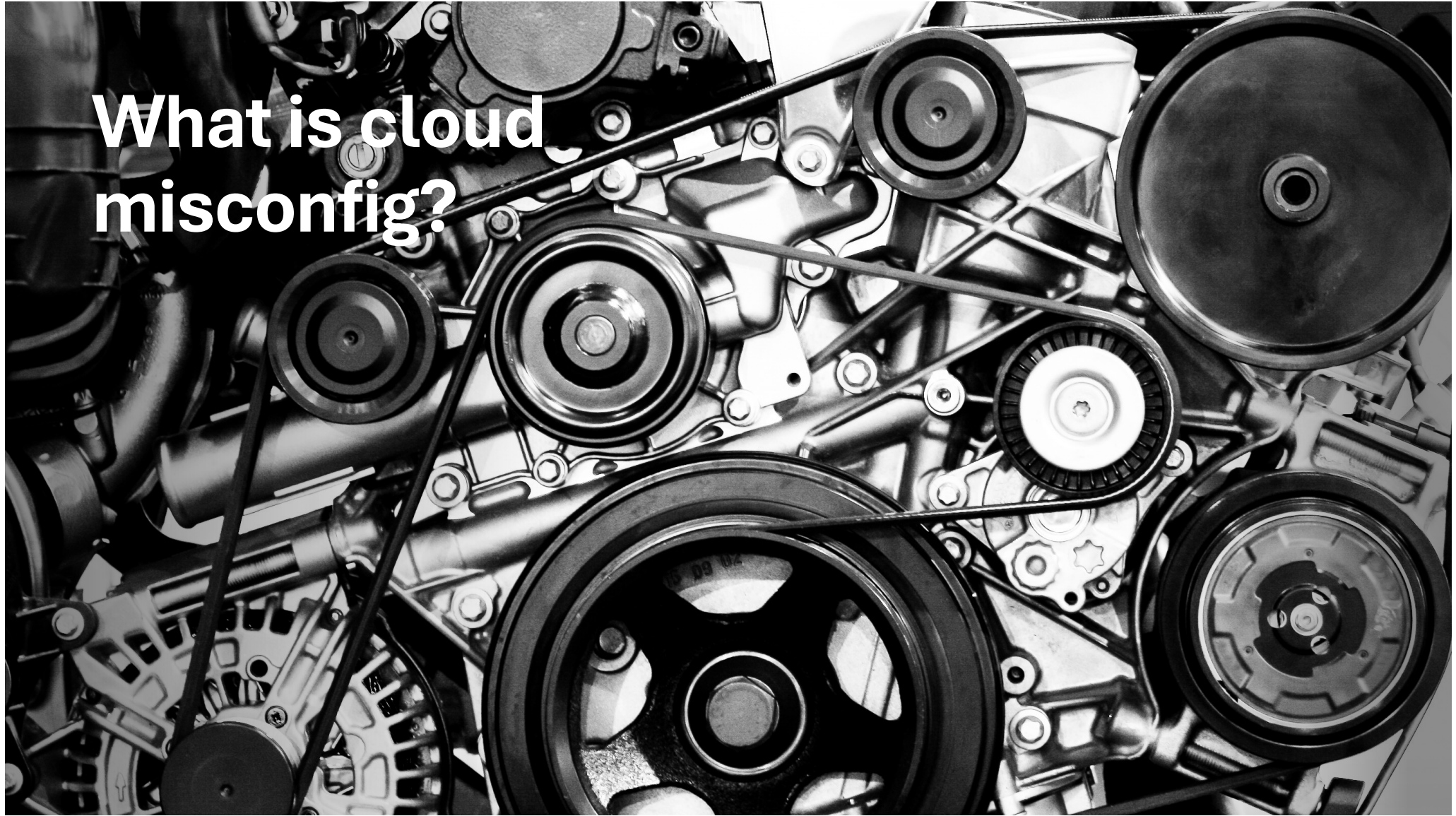
Impact=Business Criticality

Risk = Likelihood **X** Impact

Likelihood=Vulnerabilities, Threats, Exposures, Security Controls



**What is cloud
misconfig?**



Public Accessibility

- **Public Accessibility:**
- **Description:** Buckets or files are set to be publicly accessible without requiring authentication.
- **Risk:** Anyone with the URL can access the data, leading to potential leaks of sensitive or confidential information.

Lack of Encryption:

- **Lack of Encryption:**
- **Description:** Data stored in cloud storage is not encrypted, either at rest (when stored) or in transit (when being transferred).
- **Risk:** Unencrypted data is vulnerable to unauthorized access, interception, and theft.

Improper Permissions

- **Improper Permissions:**
- **Description:** Access control policies are not correctly set, granting excessive permissions to users or services.
- **Risk:** Unauthorized users or applications can access, modify, or delete data.

Lack of Monitoring and Logging

- **Lack of Monitoring and Logging:**
- **Description:** Absence of proper monitoring and logging of access and changes to data.
- **Risk:** Lack of visibility into who accessed or modified data, making it harder to detect and respond to breaches.

Weak Authentication and Authorization

- **Weak Authentication and Authorization:**
- **Description:** Insufficient authentication mechanisms or poorly managed credentials.
- **Risk:** It can allow unauthorized access to sensitive data due to weak or compromised credentials.



What is your responsibility

Do you know your environment?
Are you ready to Decipher it?

What is Cloud computing?



Cost-efficiency

Scalability

Flexibility

Reliability

Innovation

Security

Collaboration

Introduction to cloud computing and benefits

Cloud Services Model



Security in the Cloud

Customer is responsible for managing these in their own environment (including own subscription).



Shared responsibility areas

Services are provided by Microsoft, but customer must also configure them in line with security and compliance needs.



Security of the Cloud

Microsoft or the CSP is responsible for managing privacy, security and compliance.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Customer data	Customer	Customer	Customer	Customer
Configurations and Settings	Customer	Customer	Customer	Customer
Identities and Users	Customer	Customer	Customer	Customer
Client devices	Customer	Customer	Shared	Shared
Applications	Customer	Customer	Shared	Shared
Network controls	Customer	Customer	Shared	Microsoft
Operating System	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical Datacenter	Customer	Microsoft	Microsoft	Microsoft

■ Customer
 ■ Microsoft
 ■ Shared

Action Plan for Cloud Service Model Assessment



Follow the Framework

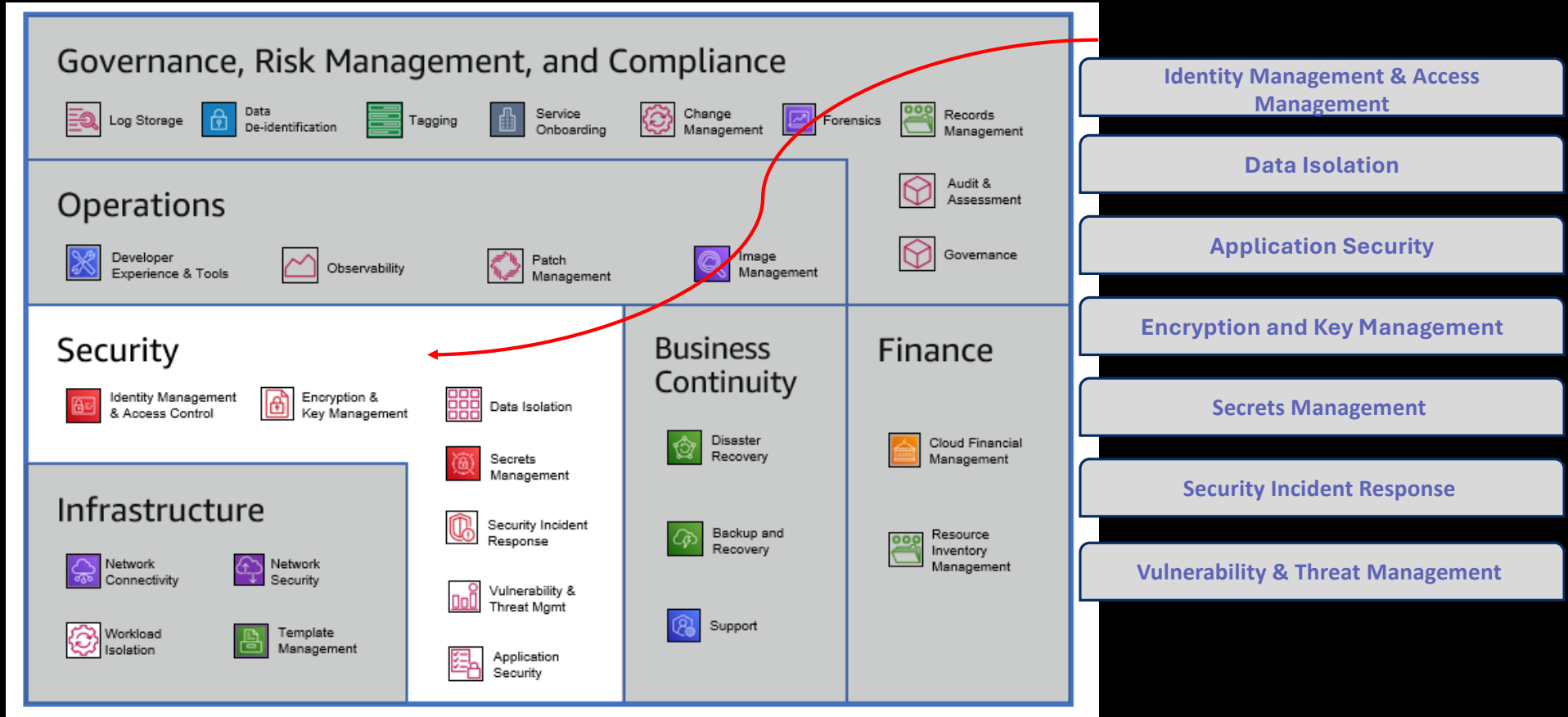
Where do I start from ?

Which framework is
the right framework
for me



https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home

Security Controls Best Practices for Cloud



Source AWS

DEMO

CSA -CCM - Control Matrix v4.04

How to use CCM

Typical Control Applicability and Ownership			Architectural Relevance - Cloud Stack Comp			
IaaS	PaaS	SaaS	Phys	Network	Compute	Storage
Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE
Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE
Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE

What to ask for?





WHAT TYPE OF BUSINESS FOR YOUR ORGANIZATION?



WHAT CLOUD SERVICE MODEL IS BEING USED?



ARE THERE INFORMATION SECURITY POLICIES RELATED TO CLOUD?



IS THERE ANY SENSITIVE DATA SUCH AS DOB, SSN, NAME, ADDRESS, LOCATION OR ANY IDENTIFIABLE DATA HOSTED IN THE CLOUD?



DO YOU HAVE DATA CLASSIFICATION DEFINED?



LOOK FOR DATA PROTECTION TOOLS AND PROCEDURE?



UNDERSTAND THE BUSINESS WHERE AND HOW DO THEY OPERATE?

Criteria - Data Security



Criteria – Identity and Access Management



What type of business for your organization?

What cloud service model is being used?

Do you have federated identities?

How many global admin accounts do you have?

How do you enforce MFA across the org including IT?

Do you have managed devices only?

Have you implemented RBAC?



Criteria – Application Security



What type of business for your organization?

What cloud service model is being used?

Are you fully hosted (apps) in the cloud?

Are there any applications deals with sensitive data?

Do you perform application security testing?

Do you have change management in your product development?

Thank You

Sign up for a onetime free
mentorship session

<https://forms.office.com/r/uBDb6RAuLN>

