TechLift

KICKSTART YOUR CAREER

Cloud Computing Basics
What, why, & how

P@SHA
Pakistan Software Houses Association for IT & ITES

PAKISTAN
PSEB
SOFTWARE EXPORT BOARD

S. No.	Topics
1	What's in it for you? Before Cloud Computing About Hypervisors and virtualization
2	What is cloud computing? Types of Cloud Computing Public Cloud Private Cloud Hybrid Cloud IP Addressing with Types
3	Cloud Architecture Benefits IaaS, PaaS, SaaS
4	Benefits Of Cloud Computing
5	Cloud Management
6	Microservices Architecture How MicroServices Works? Benefits Microservices Challenges of MicroServices Characteristics of MicroServices MicroServices in Cloud Benefits of using Microservices in cloud

S. No.	Topics
7	Cloud VS on-prem Security Introduction On-prem Security Benefits Cost of On-prem Security Benefits of Cloud Security Cons of Cloud Security
8	Cloud Computing Security Deep Dive What is Cloud Security Principal of Cloud Computing Security Cloud Computing Security Best practice
9	Module Review AWS Certification Road Map Azure Certification Road Map

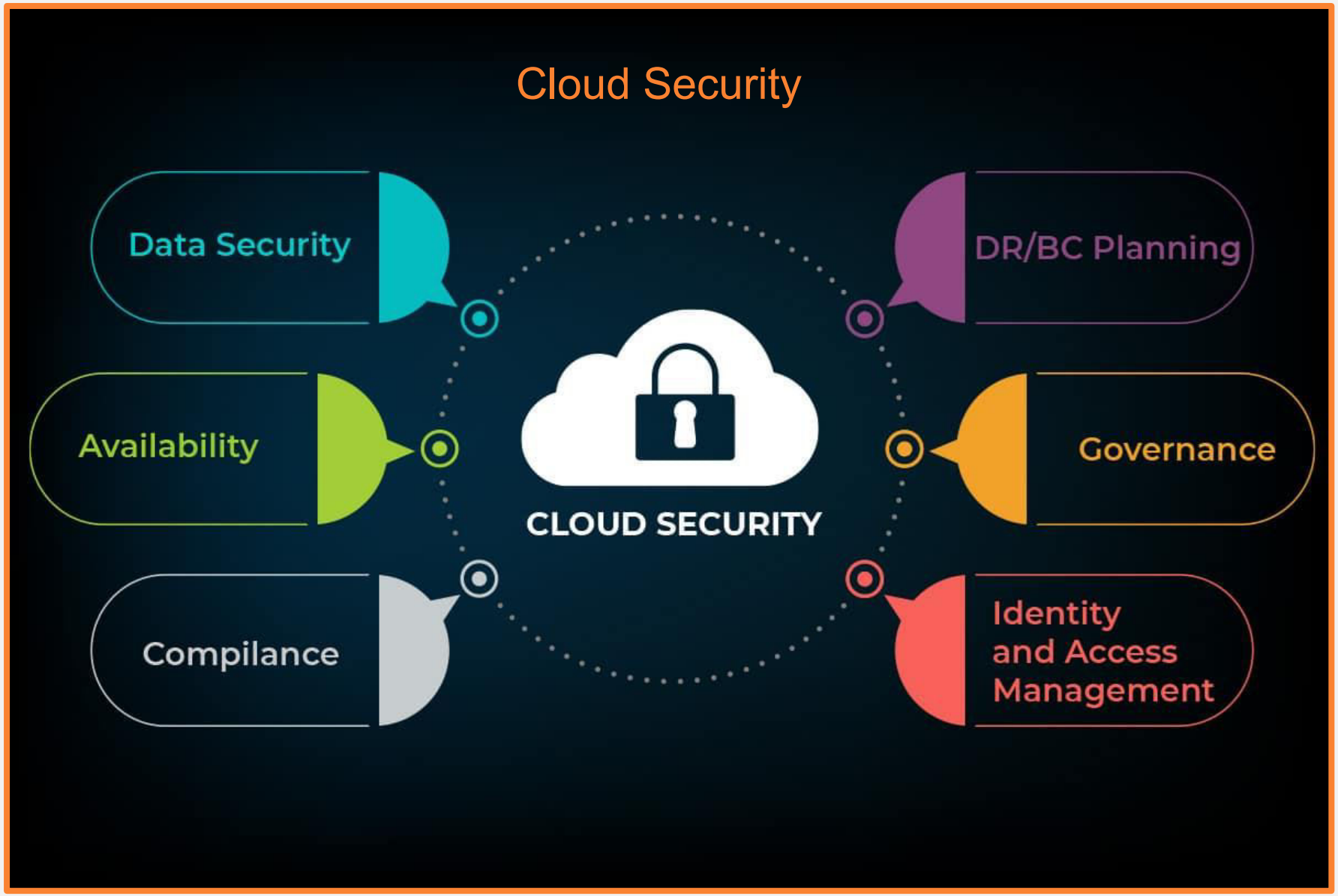
TechLift

KICKSTART YOUR CAREER

Cloud vs On-Prem Security

P@SHA
Pakistan Software Houses Association for IT & ITES

PAKISTAN PSEB SOFTWARE EXPORT BOARD


Cloud Security
Data Security
DR/BC Planning
Availability
Governance
CLOUD SECURITY
Compilance
Identity and Access Management

On Prem Vs Cloud Securtiy:

- The on-prem versus cloud security debate continues within the data center industry.
- The differences range from minor to substantial, but both on-prem and cloud advocates can agree that countless protections and threats exist in either environment.
- Beyond focusing solely on meeting IT security priorities.

The Question Is: **Which is more secure for my organization and its business objectives?**

On-Prem Securtiy:

On-premises servers are the traditional enterprise computing model. In this implementation, all hardware and software resides in house.

A business purchases and maintains its own servers, located in a secure, climate-controlled room onsite.

The company needs specialized IT support to manage the equipment, as well as appropriate HVAC systems, UPS, battery powers etc to keep the equipment in working order.

IT professionals must stay up-to-date with the latest software updates and perform regular backups. A continuous expansion in business needs to procure new hardware to meet its growing demands.

On-Prem Securtiy:

Benefits Of On-Prem Security:

- **Increased Control**
  More control over security is retained when a company manages services with its own on-prem servers.

- **Infinite Customization**
  On-Premises serves to allow network customization that is tailor-made for a company's needs.

- **More Reliable**
  On-prem servers do not rely on an internet connection.

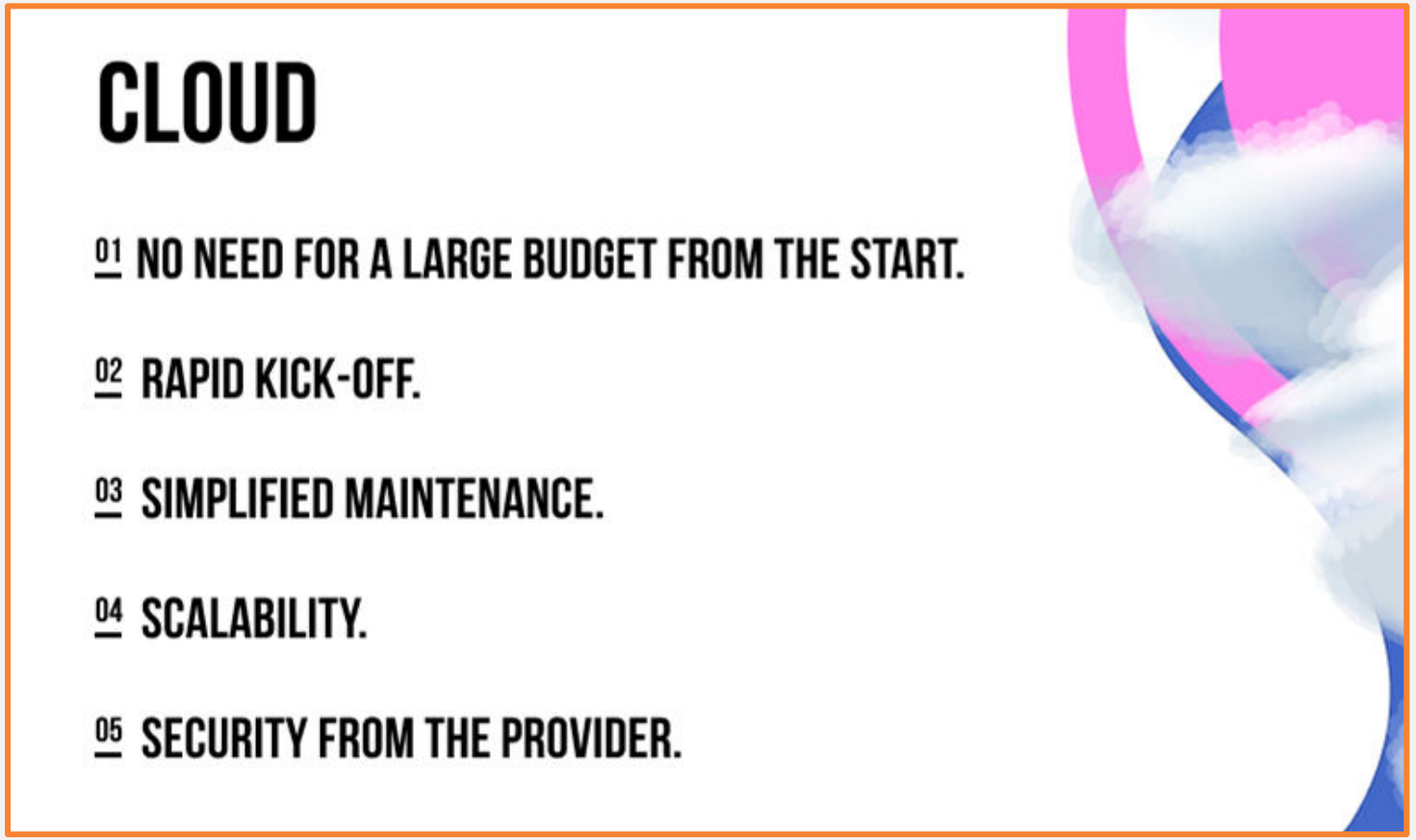
- **Quicker Learning Curve**
  The majority of IT professionals are better equipped to build security processes in this environment.

Cons Of On-Prem Security:

- **Timely To Scale**
  Procurement of IT hardware can take time and research to scale security for on-prem data centers.

- **Increases The Need For On-Site Security**
  Without the right team and safety controls in place, some businesses may be more vulnerable to physical threats such as damage to physical property.

Cloud Securtiy:



Benefits Of Cloud Securtiy:

- **Easier To Scale**
  Expanding storage for data in the cloud is as straightforward as upgrading a cloud storage package.

- **Faster Set-Up**
  Cloud-based security is more automated, which means set-up takes minutes rather than days.

- **Flexible Pricing Structure**
  Cloud computing often has a more flexible pricing structure with “pay-as-you-grow” fees.

Cons Of Cloud Securtiy:

- **Increased Vulnerabilities**
  The cloud's larger attack surface can make it particularly vulnerable to cyberattacks.

- **Limited Customization**
  Traditional monitoring and security tools do not always work in cloud environments.

- **Regulation Issues**
  Some regulations require that the shared responsibility of multi-tenant hardware is not used.

- **More Expensive**
  Cloud computing often has a more flexible pricing structure with "pay-as-you-grow" fees, but is less predictable for forecasting unforeseen costs and is more expensive in the long term.

	On-premise	Cloud
Installation	You manage	Automatic
Firewalls	You configure	Automatic
IT infrastructure	You provide	Included
Database security	You provide	Included
Virus protection	You provide	Included
Patches/ Updates	Manual	Included
Upgrades	Manual	Included
24/7 monitoring	You provide	Included
Mobile CMMS	You configure (if possible)	Included

SECURITY

CLOUD SECURITY

- Cloud provider is responsible for security on an equal footing with the client
- Security is automated, thanks to the presence of various APIs
- Adding additional features and requirements entails an increase in the cost of the cloud provider's services
- Some conditions in the work of the provider are immutable and may not suit you
- An initial investment in security is zero - this is included in the cost of the entire service
On-Premise Security

ON-PREMISE SECURITY

- Fully implemented by company resources
- Provides the need to ensure offline security too
- The high initial investment, but without the need for constant infusion of funds
- Custom server configuration for the specific needs of your business
- All control on your part

Q&A Session

1. During which phase of a cloud migration framework is security the most critical?
    a. Discovery phase
    b. Cloud migration phase
    c. Operations phase
    d. All of the above

1. Cloud security analytics can help enterprises:
    b. Predict account hijacking
    c. Detect malware with unknown signatures
    d. Monitor data for access
    e. All of the above

What we achieved?

Introducing the Cloud
Hypervisors
Types Of Cloud
Architecture of Cloud
Microservices
Cloud Security
AWS Certification RoadMap
Azure Certification RoadMap