CCSP

CCSP EXAM CRAM

EXAM PREPARATION SERIES

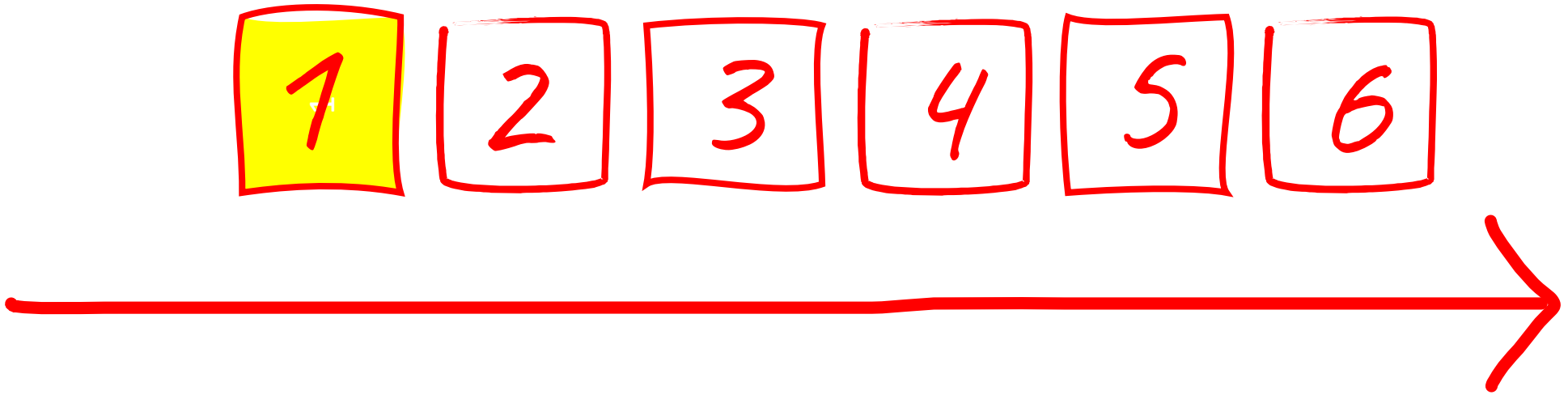
2023 EDITION

DOMAIN 1

And exam prep strategy to take you *further, faster*!

with **Pete Zerger** vCISO, CISSP, MVP

LESSONS IN THIS SERIES



One lesson for each exam domain

...and a consolidated full course video when the series is complete

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1. Cloud Concepts, Architecture, and Design	**17%**
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk, and Compliance	13%

Domain 1 is the focus of this video

CCSP

EXAM STUDY GUIDE

& PRACTICE TESTS BUNDLE

BUY IT NOW AT amazon.com

Link to the latest exam bundle in the video description !

EXAM DETAILS

Last update	August 1, 2022
Number of question	150 (*includes 50 unscored pre-test questions*)
Types of questions	Multiple-choice
Length of test	4 hours
Experience requirements	▪ Candidates must have a minimum of 5 years cumulative paid work experience in information technology ▪ 3 years must be in information security ▪ And 1 year in 1 or more of the 6 domains of the CCSP CBK.

HOWEVER

Earning (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement!

Link to my CISSP Exam Cram in video description!

EXAM DETAILS

Last update	August 1, 2022
Number of question	150 (*includes 50 unscored pre-test questions*)
Types of questions	Multiple-choice
Length of test	4 hours
Experience requirements	▪ Candidates must have a minimum of 5 years cumulative paid work experience in information technology ▪ 3 years must be in information security ▪ And 1 year in 1 or more of the 6 domains of the CCSP CBK.
Passing score	700 of 1000 points


There is no
AWARD
for the longest
STUDY TIME!

CSSP EXAM CRAM

THE COMPLETE COURSE

EXAM PREP

Recommended Exam Preparation Strategy

INSIDE CLOUD AND SECURITY

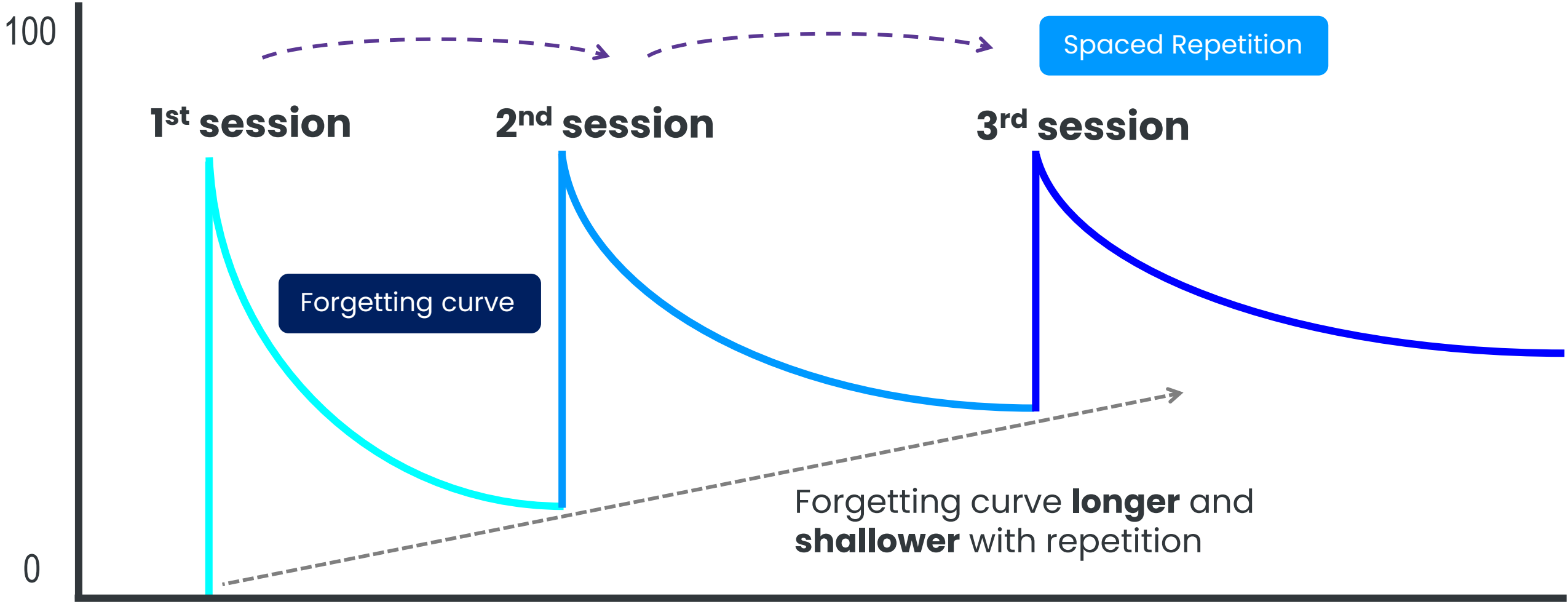
20 min

24 hours

1 week

THE POWER OF REPETITION

SPACED REPETITION



HOW LONG DOES IT TAKE TO MEMORIZE ANYTHING?

TO MEMORIZE QUICKLY

short-term

1st repetition	Right after learning
2nd repetition	After 20-30 min
3rd repetition	After 1 day
4th repetition	After 2-3 weeks
5th repetition	After 2-3 months

1st repetition	Right after learning
2nd repetition	After 15-20 min
3rd repetition	After 6-8 hours
4th repetition	After 24 hours
5th repetition	After 48 hours

TO MEMORIZE FOR A LONG TIME

EXAM PREP STRATEGY

Research shows everyone benefits from a variety of sources!

TARGETED READING

PRACTICE EXAMS

LIVE QUIZ (or flashcards)

POWERPOINT REVIEW

VIDEO CONTENT

Mix, match, and repeat based on your preferences

EXAM PREP STRATEGY

Research shows everyone benefits from a variety of sources!

TARGETED READING?

PRACTICE EXAMS

LIVE QUIZ (or flashcards)

POWERPOINT REVIEW

VIDEO CONTENT

Use OSG for topics you are struggling with...

EXAM PREP STRATEGY

Research shows everyone benefits from a variety of sources!

TARGETED READING?

PRACTICE EXAMS

LIVE QUIZ (or flashcards)

POWERPOINT REVIEW

VIDEO CONTENT

...but not to read cover-to-cover!

UNDERSTANDING CONCEPTS

Studies show understanding **BEFORE** you memorize greatly improves retention

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 1

Cloud Concepts, Architecture & Design

I will cover every topic mentioned in the exam syllabus!

INSIDE CLOUD AND SECURITY

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 1

Cloud Concepts, Architecture & Design

I will also provide examples of concepts when possible

INSIDE CLOUD AND SECURITY

EXAM ESSENTIALS - DOMAIN 1

Critical exam topics according to the Official Study Guide (OSG)!

Explain the different roles in cloud computing

Service Providers, Service Partners, Access Service Brokers, Regulators

Identify the key characteristics of cloud computing

On-demand self-service, multitenancy, elasticity, scalability, resource pooling, etc.

Explain the three cloud service categories

IaaS, PaaS, SaaS

Describe the five cloud deployment models

Public, Private, Hybrid, Community, Multi-cloud

Identify important related technologies

Machine Learning, Artificial Intelligence, Blockchain, DevSecOps, Quantum, Edge, Fog

Explain shared considerations in the cloud

Interoperability, Portability, Privacy, Security, Resiliency, Governance, Versioning, etc.

1. CLOUD CONCEPTS, ARCHITECTURE, AND DESIGN

1.1 Understand Cloud Computing Concepts

Cloud Computing Definitions

Cloud Computing Roles and responsibilities
(e.g., cloud service customer, cloud service provider, cloud service partner, cloud service broker)

Key Cloud Computing Characteristics
(e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)

Building Block Technologies
(e.g., virtualization, storage, networking, databases, orchestration)

NIST SP 800-145

Cloud computing is a model for enabling universal, convenient, on-demand network access …

to a shared pool of configurable computing resources…

(e.g., networks, servers, storage, apps, and services)

…that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The NIST definition of cloud computing

CLOUD COMPUTING ROLES

Provider

Cloud Service Provider

CSP

Company that provides cloud-based platform, infrastructure, and applications to other organizations as a service.

(e.g., Amazon (AWS), Msft Azure, Google (GCP)

Partner

Cloud Services Partner

Help organizations to obtain and deploy cloud services.

May provide consulting services, software to run in the cloud, or both.

(e.g., Avanade, Tata, Accenture)

CLOUD COMPUTING ROLES

Customer

User/subscriber of cloud services

The business or individual consuming cloud services

Often using cloud to complement / augment existing on-premises compute

CSA

Cloud Service Auditor

Third party that can conduct an independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.

Audit scope may vary, "independent assessment" is key

CLOUD BROKER

an entity that manages the use, performance and delivery of cloud services

negotiates relationships between cloud providers (CSPs) and cloud consumers.

Serves as an intermediary (advisor, negotiator) between customer and CSP

Functions of a Cloud Broker

Service Intermediation

enhances a given service by improving specific capabilities and providing value-added services to cloud consumers.

Service Aggregation

combines and integrates multiple services into one or more new services.

Service Arbitrage

means a broker has the flexibility to choose services from multiple agencies.

Other cloud computing roles

Less likely to appear on the exam, but just in case...

Cloud administrator. Implementation, monitoring, and maintenance of the cloud.

Cloud application architect. Adapting, porting, and deploying application.

Cloud architect. Designs and develops solutions.

Cloud operator. Responsible for daily operational tasks.

Cloud data architect. Manages data storage and data flow within, to and from the cloud.

Other cloud computing roles

Less likely to appear on the exam, but just in case...

Cloud service manager. Responsible for business agreement, pricing for the cloud customer.

Cloud storage administrator. Manages storage volume/repository assignment and configuration.

Cloud service business manager. Oversees business and billing administration.

Cloud service operations manager. Prepares systems operations and support for the cloud, administers services.

CLOUD COMPUTING ROLES

MSSP

Managed Security Service Provider

maintains the security environment for companies

may manage firewalls, IDPS, and SIEM systems, and other security services and infrastructure.

may provide an outsourced security operations center (SoC) and incident response

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

On-demand self-service

Customers can scale their compute and storage needs with little or no intervention or prior communication from the provider.

Technologists can access cloud resources almost immediately when they need to do their jobs, providing agility in service delivery.

Broad network access

Services are consistently accessible over the network regardless of the users physical location .

KEY CLOUD COMPUTING CHARACTERISTICS

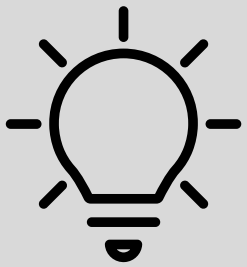
Characteristics common in cloud platforms and services

Multitenancy

Which means many different customers share use of the same computing resources.

Physical servers that support our workloads might be the same physical servers supporting other customers' workloads.

The underlying cloud infrastructure (compute, storage, networking) is shared. (by multiple customers)



Oversubscription:
Cloud providers will oversubscribe their total capacity, meaning they'll sell more capacity than they have.

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

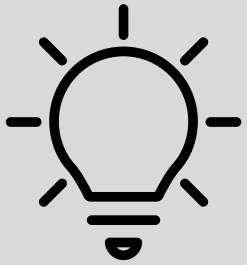
Multitenancy

True in IaaS, PaaS, SaaS and scenarios

Which means many different customers share use of the same computing resources.

Physical servers that support our workload might be the same physical servers supporting other workloads.

The underlying cloud infrastructure (compute, storage, networking) is shared.



Oversubscription:
Why? Because in the big picture customers won't be collectively using all of that capacity simultaneously.

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

Rapid elasticity and scalability

Allows the customer to grow or shrink the IT footprint as necessary to meet needs without excess capacity.

These two are related, but unique. What's the difference?

Elasticity. The ability of a system to **automatically grow and shrink** based on **app demand**.

Capabilities can be rapidly provisioned and de-provisioned (scale-out, scale-in)

Additional instances quickly auto-deployed

Scalability. The ability of a system to handle growth of users or work. Ability to grow as demand increases.

Controlled by SKU or tier selection

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

Resource pooling

Enables cloud provider to apportion resources as needed across multiple customers so resources are not underutilized or overtaxed.

Enables cloud provider to make capital investments that greatly exceed what any single customer could provide on their own.

Allows the cloud provider to meet various demands from customers while remaining financially viable.

DISADVANTAGE: Can result in some degree of location dependence beyond customer control.

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

Resource pooling

Enables cloud provider to apportion resources as needed across multiple customers so resources are not underutilized or overtaxed.

Enables cloud provider to make capital investments that greatly exceed what any single customer could provide on their own.

Allows the cloud provider to meet various demands from customers while remaining financially viable.

Important in data residency compliance!

However, major CSPs (AWS, Azure, GCP) often provide options enabling customers to choose location.

KEY CLOUD COMPUTING CHARACTERISTICS

Characteristics common in cloud platforms and services

Measured service aka "metered service"

means that almost everything you do in the cloud is metered (measured and tracked) for management and billing purposes.

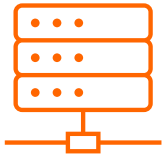
COMMON METRICS

Cloud providers measure metrics, of resource consumption, like:

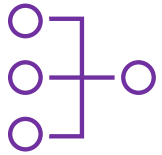
- ✓ number of minutes of virtual server compute time
- ✓ Amount of disk space you consume
- ✓ Number of function calls you make
- ✓ Amount of network egress and ingress

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

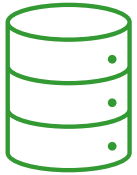


Compute

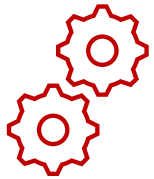


Network

Storage



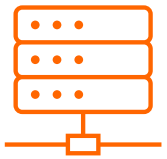
Databases



Orchestration

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:



Compute

Infrastructure-as-a-Service (IaaS) is the basis for compute capacity in the cloud.

CSP provides the server, storage, and networking hardware and its virtualization.

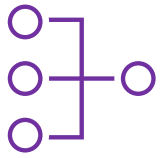
Customer installs middleware and applications.

Customer only pays for what they use. Charges stop when instance is stopped or deleted.

See "shared responsibility model" later in Domain 1.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:



Network

Cloud networking is all virtualized to allow customers to design and customize to their needs.

Enables customers to segment networks and restrict access however they would like.

Physical network components are virtualized into a **software-defined network (SDN)**.

Examples: Azure VNET, AWS VPC, GCP VPC

STORAGE DEFINED NETWORK (SDN)

A network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software

SDN is defined by **three** separate planes or layers:

Management plane: the business applications that manage the underlying control plane are exposed with northbound interfaces.

Control plane: Control of network functionality and programmability is made directly to devices at this layer.

OpenFlow was the original framework/protocol at the control plane

Data plane: The network switches and routers located at this plane are associated with the underlying network infrastructure.

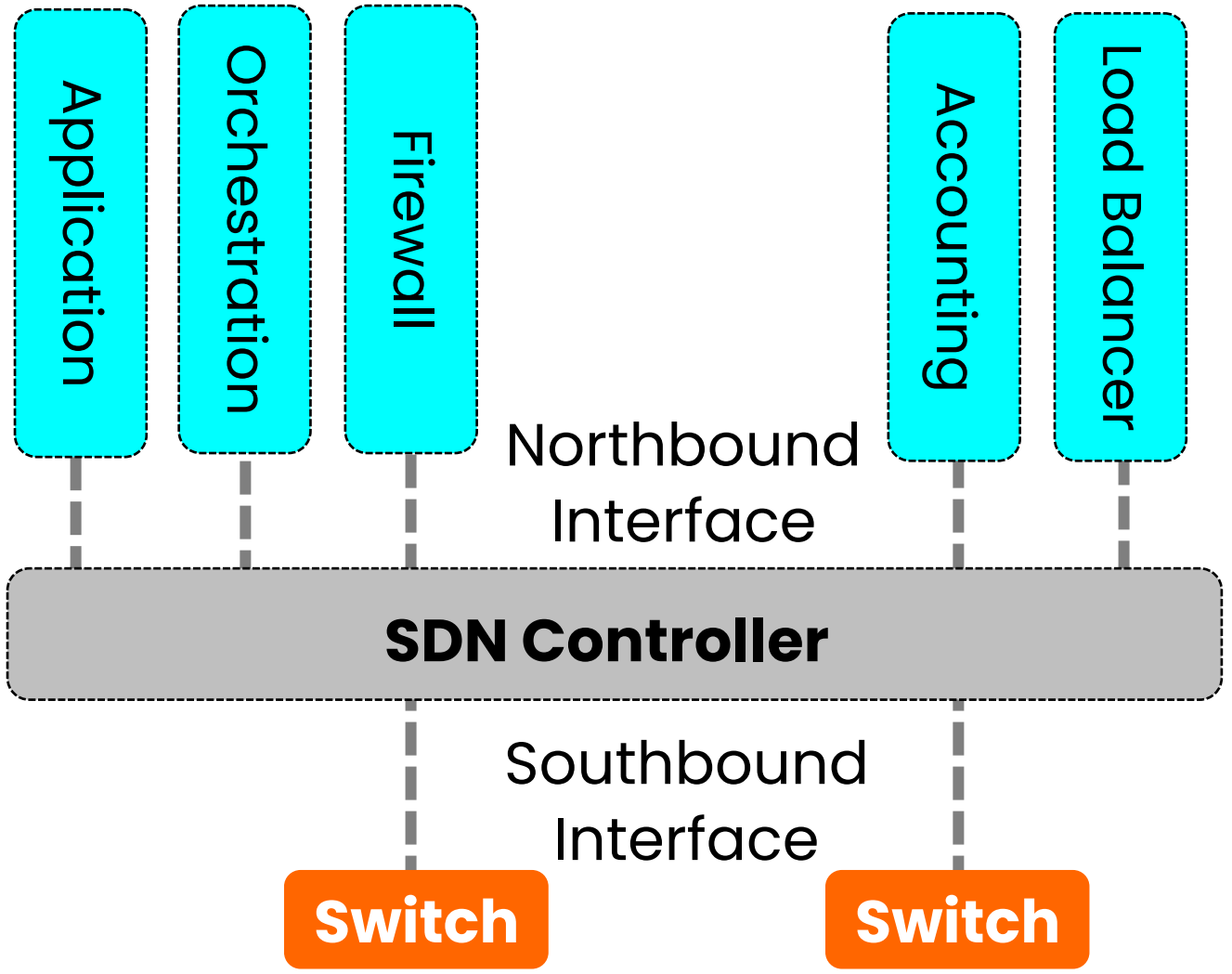
Data forwarding happens here, so also known as 'Forwarding plane'

STORAGE DEFINED NETWORK (SDN)

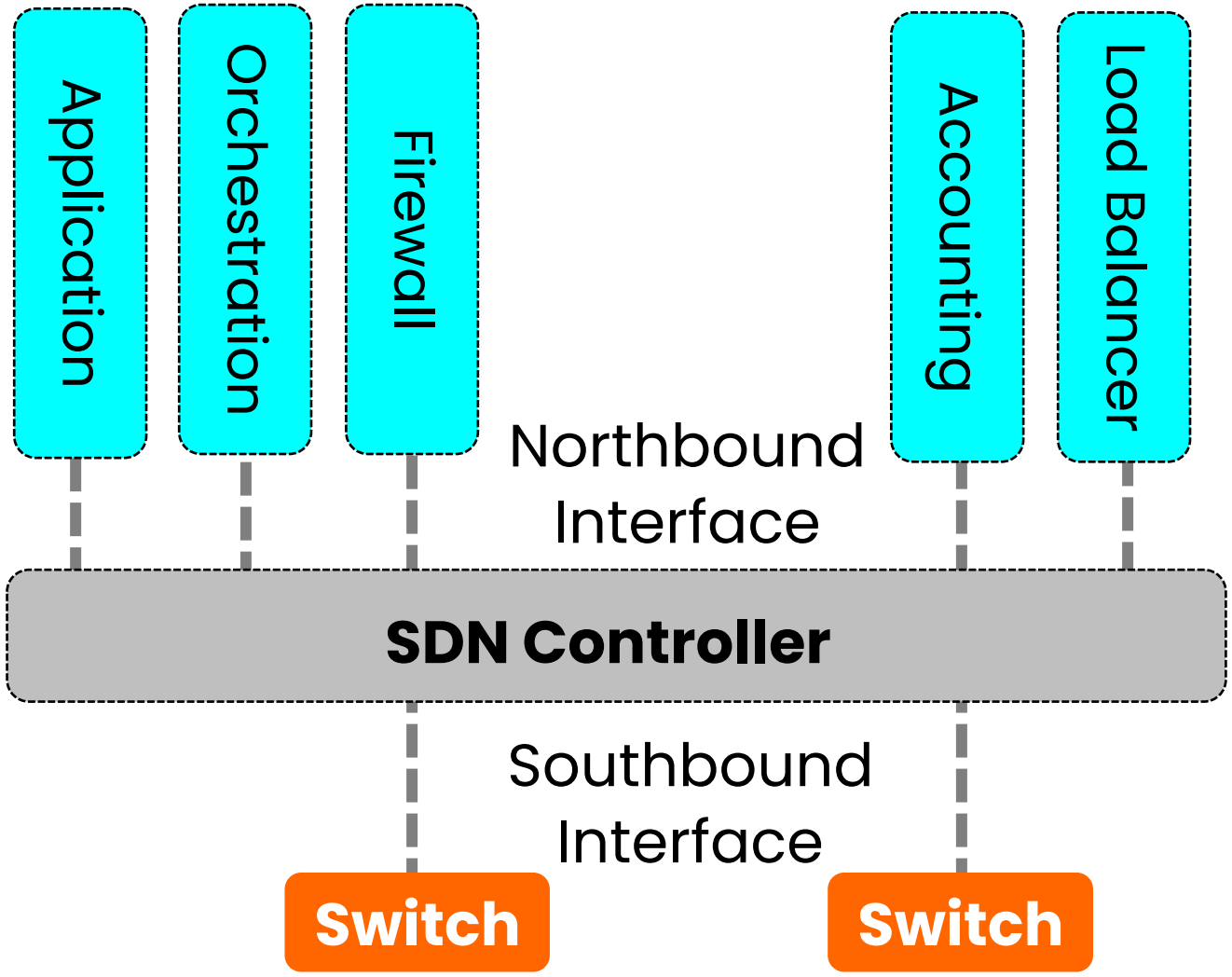
Management Plane

Control Plane

Data Plane



STORAGE DEFINED NETWORK (SDN)



Northbound interface ensures only trusted, authorized applications access critical network resources.

OpenFlow protocol interfaces with devices through **southbound interfaces**.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

IaaS

Exam considers three types of storage: **long-term**, **ephemeral**, and **raw**.

Ephemeral is relevant for IaaS instances and exists only as long as the instance (VM) is up.

Raw storage maps a logical unit number (LUN) on a storage area network (SAN) to a VM.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

IaaS

Long-term storage offered by some CSPs is tailored to the needs of data archiving.

This may include features like search, immutability, and data lifecycle management.

Long term storage typically use either **Volume** or **Object** storage infrastructure.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

IaaS

Long term storage typically use either **Volume** or **Object** storage infrastructure.

Examples of **volume** (block) storage include Amazon EBS and Azure Disk Storage.

Examples of **object** storage include Amazon S3 and Azure Blob Storage.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

PaaS

Databases, usually multitenant relational (SQL) databases as a service.

Examples: MSSQL, MySQL, PostgreSQL

Big data as a service, nonrelational (NoSQL) data, such document, graph, column, or key-value

Examples: MongoDB, Cassandra, HBase

Storage Consistency

a fundamental concept that describes the time it takes for all data copies to be the same.

Strict consistency

ensures that all copies of the data have been duplicated among all relevant copies before finalizing the transaction to increase availability.

Eventual consistency

consistency of data is relaxed, which reduces the number of replicas that must be accessed during read and write operations before the transaction is finalized.

Data changes are 'eventually' transferred to all data copies via asynchronous propagation over the network

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

SaaS

Content/file storage: File-based content stored within the application

Content delivery network (CDN) where content is stored in object storage, then replicated to multiple geographically distributed nodes to improve internet consumption speed

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:

Storage varies by model (IaaS, PaaS, SaaS)

Storage

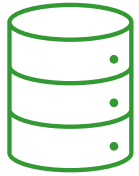
SaaS

Information storage and management: Data entered into the system via the web interface and stored within the SaaS application.

Often utilizes databases, which in turn are installed on object or volume storage.

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:



Databases

Multiple options available and multiple flavors of relational (SQL) and non-relational (NoSQL).

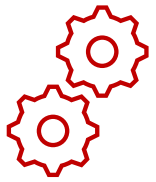
Managed database services (PaaS) options shift infrastructure maintenance to the CSP.

IaaS (VM) hosted databases are an option where PaaS is not possible or practical.

Examples: Azure DB for MSSQL, MySQL, or PostgreSQL, Amazon RDS, Amazon DynamoDB

BUILDING BLOCK TECHNOLOGIES

The **5 building block technologies** of the cloud:



Orchestration

Cloud orchestration creates automated workflows for managing cloud environments.

Builds on the foundation of Infrastructure as Code (IaC), reducing manual admin tasks.

May be a script, function, runbook, or developed in an external workflow engine.

Examples: Azure Automation, AWS Systems Manager or 3rd parties like Zapier

VIRTUAL ASSETS

Virtual assets include:

- virtual machines (VM)
- virtual desktop infrastructure (VDI)
- software-defined networks (SDN)
- virtual storage area networks (SAN)

compute
network
storage

Hypervisors are the primary component that manages virtual assets, but also provide attackers with an additional target.

Both hypervisors and VMs need to be patched

VIRTUAL ASSETS

Security issues with cloud-based assets

Storing data in the cloud increases the risk, so steps may be necessary to protect the data, depending on its value.

When leasing cloud-based services, you should know who is responsible for maintenance and security.

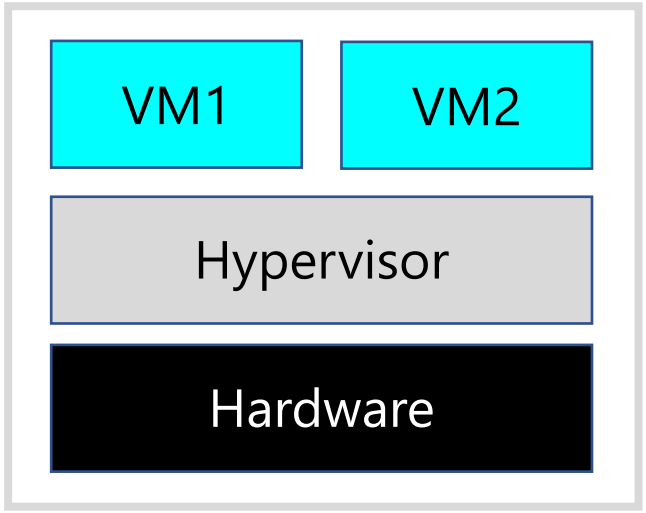
"shared responsibility model"

The **cloud service provider (CSP)** provides the least amount of maintenance and security in the IaaS model.

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"

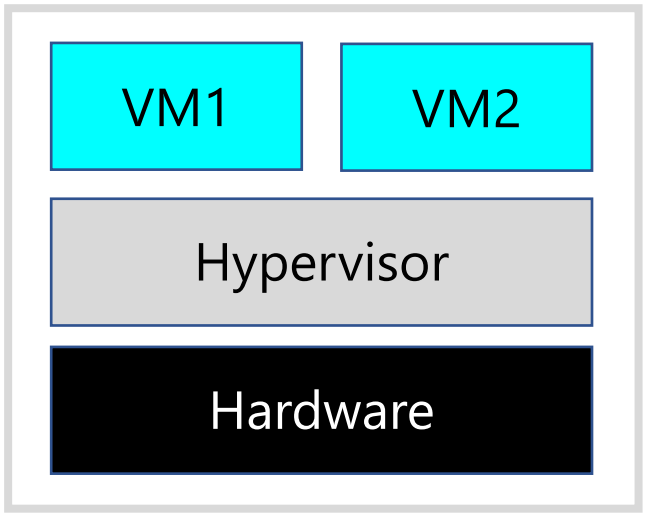


VMware ESXi, KVM
Microsoft Hyper-V

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

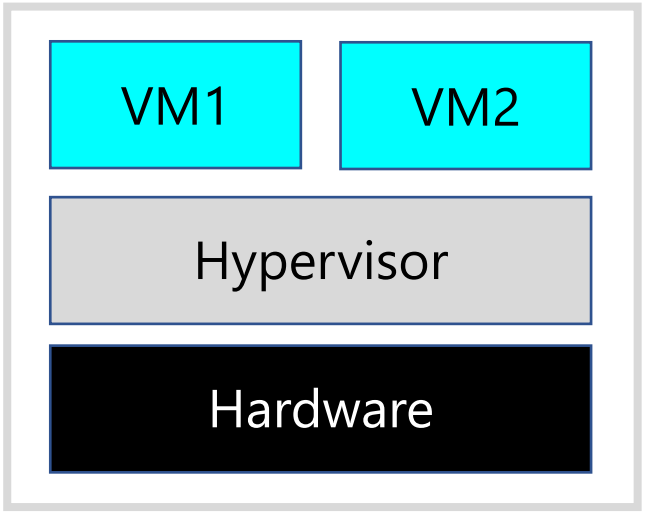
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

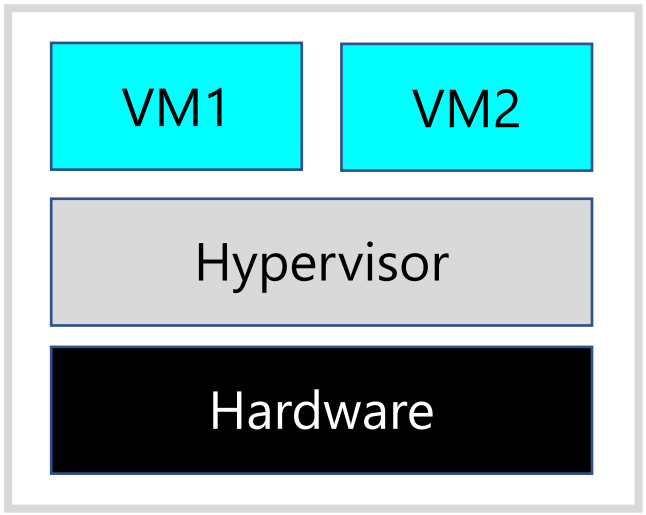
"Hosted"



BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

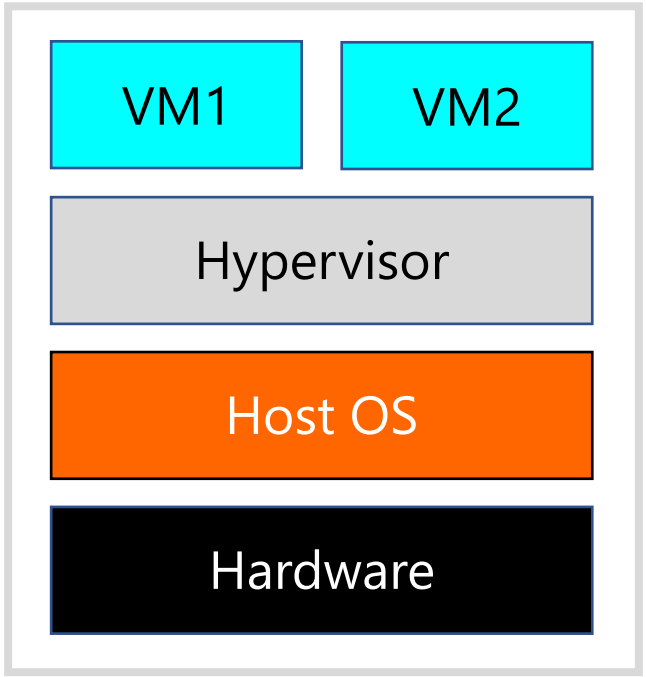
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

"Hosted"

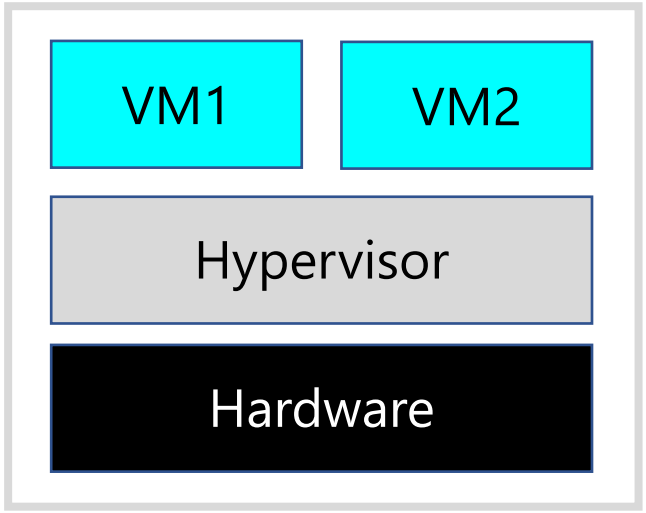


VMware Workstation,
Oracle Virtualbox

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

CHARACTERISTICS

Reduced attack surface (compared to a Type 2 hypervisor)

This makes it more secure if implemented properly

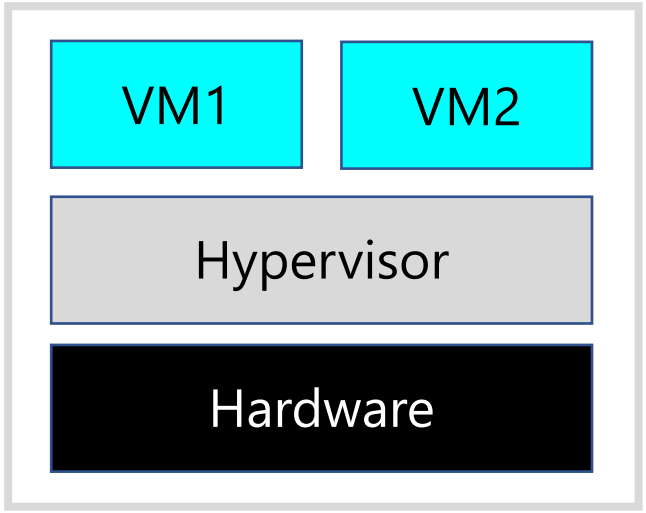
Commonly used for QA, load testing, and production scenarios

Typically, more expensive than a Type 2 hypervisor

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

CHARACTERISTICS

Increased attack surface (due to the host operating system)

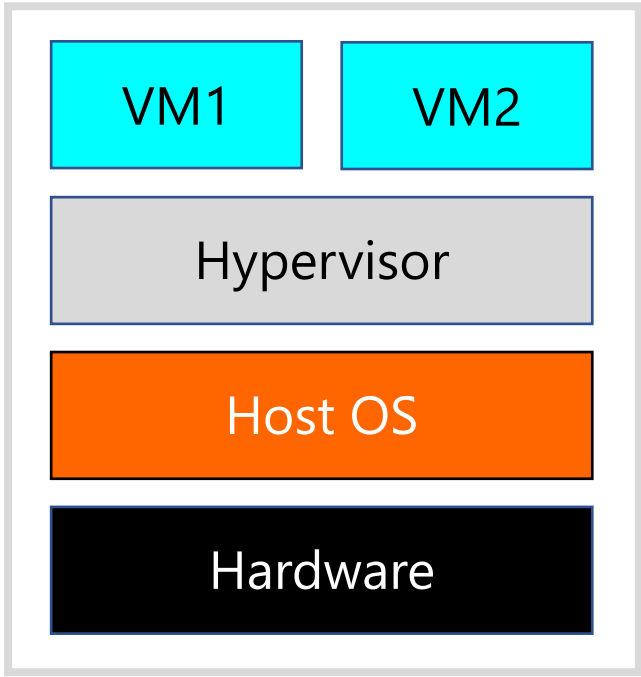
This makes it less secure vs Type 1, even if implemented properly

Commonly used for individual development and lab scenarios

Typically, less expensive than a Type 1 hypervisor

TYPE 2

"Hosted"



VMware Workstation, Oracle Virtualbox

1. CLOUD CONCEPTS, ARCHITECTURE, AND DESIGN

1.2 Describe Cloud Reference Architecture

Cloud Computing Activities

Cloud Service Capabilities
(e.g., application capability types, platform capability types, infrastructure capability types)

Cloud Service Categories
(e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

Cloud Deployment Models
(e.g., public, private, hybrid, community, multi-cloud)

Cloud Shared Considerations
(e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and Service Level Agreements (SLA), auditability, regulatory)

Impact of Related Technologies
(e.g., data science, machine learning, artificial intelligence, blockchain, Internet of Things (IoT), containers, quantum computing, confidential computing, DevSecOps)

CLOUD COMPUTING ACTIVITIES

CUSTOMER RESPONSIBILITIES

According to **ISO 17789 Cloud Reference Architecture**, the following activities are responsibilities of the **customer**:

- ✓ Use cloud services
- ✓ Perform service trials
- ✓ Monitor services
- ✓ Administer service security
- ✓ Provide billing and usage reports
- ✓ Handle problem reports
- ✓ Administer tenancies
- ✓ Perform business administration
- ✓ Select and purchase service
- ✓ Request audit reports

CLOUD COMPUTING ACTIVITIES

CSP RESPONSIBILITIES

According to **ISO 17789 Cloud Reference Architecture**, the following activities are responsibilities of the **cloud service provider**:

- ✓ Prepare systems and provide cloud services
- ✓ Monitor and administer services
- ✓ Manage assets and inventories
- ✓ Provide audit data
- ✓ Manage customer relationships
- ✓ Handle customer requests
- ✓ Perform peering with other cloud service providers
- ✓ Ensure compliance
- ✓ Provide network connectivity

CLOUD COMPUTING ACTIVITIES

PARTNER RESPONSIBILITIES

According to ISO **17789 Cloud Reference Architecture**, the following activities are responsibilities of the **cloud service PARTNERS**:

- ✓ Design, create, and maintain service components
- ✓ Test services
- ✓ Perform audits
- ✓ Set up legal agreements
- ✓ Acquire and assess customers
- ✓ Assess the marketplace

PROVIDER CSP

Delivers the cloud platform customers subscribe to and use

Microsoft, Amazon, Google

PARTNER

Provides guidance in implementing and managing customer usage of a platform

Offer services and software

CLOUD SERVICE CAPABILITIES

Capabilities, advantages, and efficiencies of public cloud

Application capability types

Overall reduction in costs, application and software licensing, reduced support costs, backend systems and capabilities.

CSP allows the customer to focus on their business use cases.

Platform capability types

Language and framework support, support for multiple environments, allowing choice and reducing "lock-in", improving ability to auto-scale.

Infrastructure capability types

Scale, converged network and shared capacity pool, self-service and on-demand capacity, high reliability and resilience.

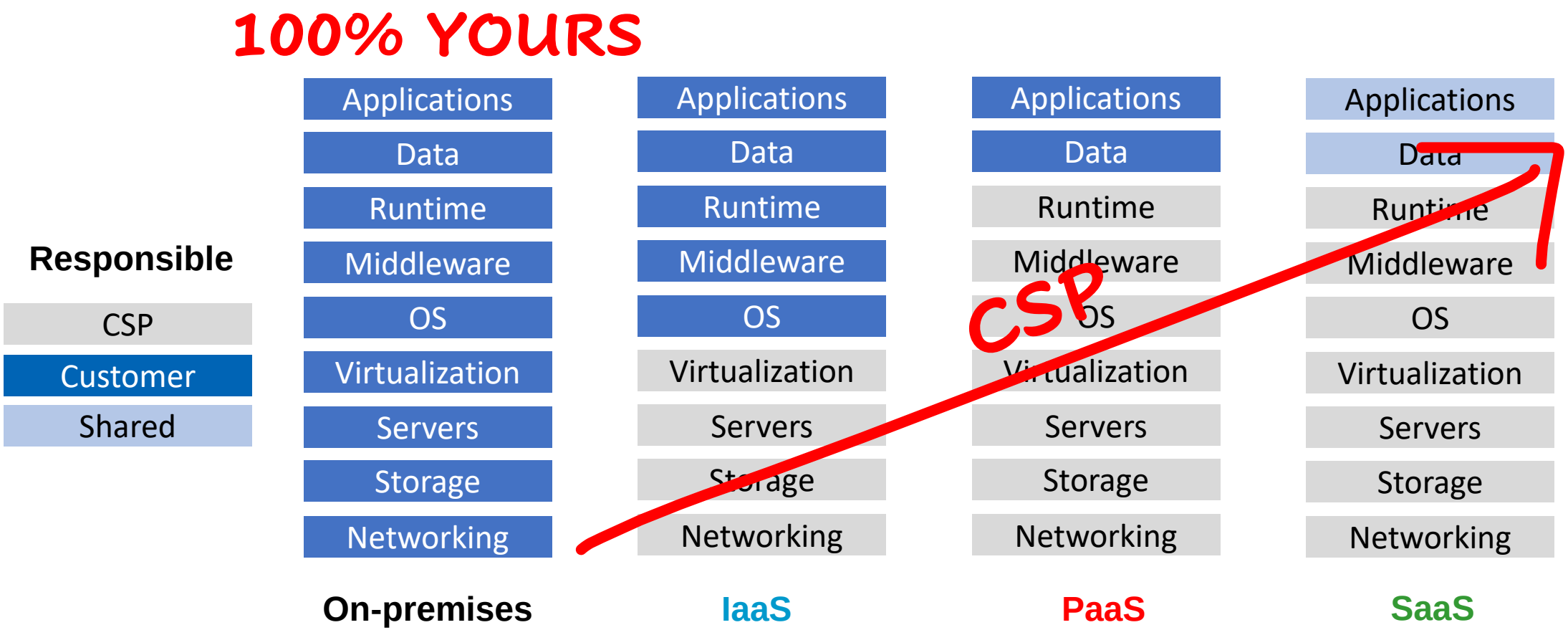
This is a capital expense (CAPEX) on-premises, but an operational expense (OPEX) in the cloud. Customer pays only for what they use.

COMPARE CLOUD

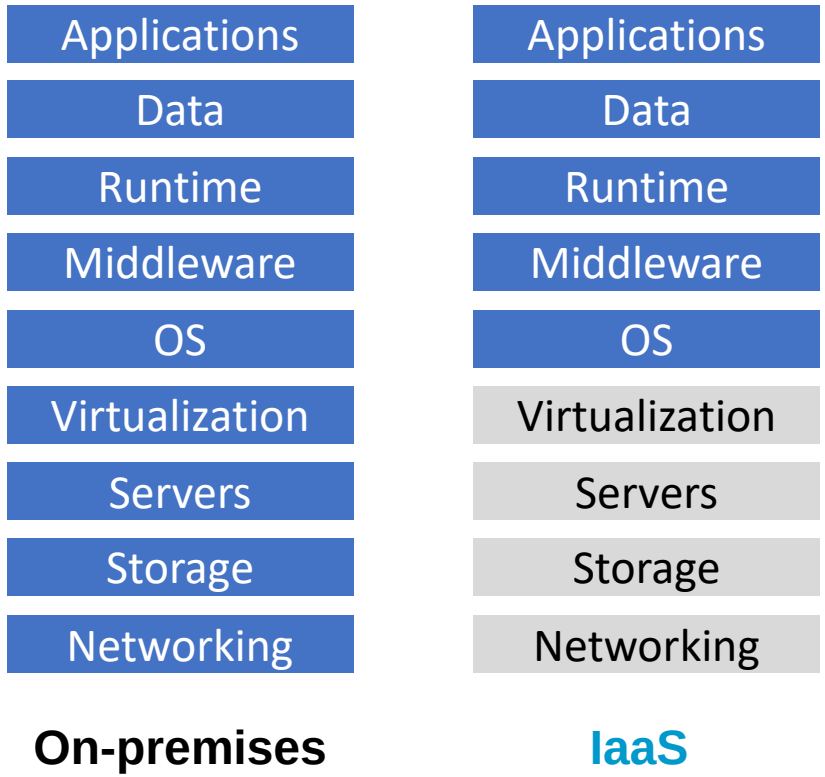
MODELS & SERVICES

SHARED RESPONSIBILITY MODEL

SHARED RESPONSIBILITY MODEL



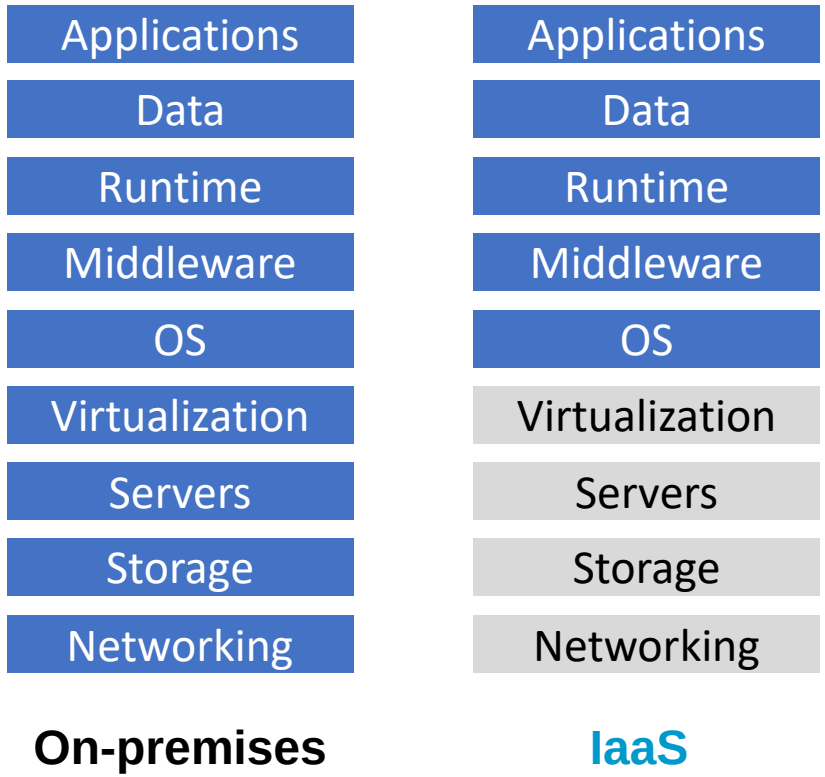
CLOUD SERVICE CATEGORIES - IAAS



CSP provides building blocks, like networking, storage and compute

CSP manages staff, HW, and datacenter

CLOUD SERVICE CATEGORIES - IAAS



Key Benefits

Usage is metered

Eases scale (scale-up, out, and down)

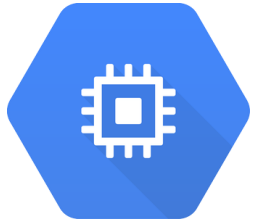
Reduced energy and cooling costs

CLOUD SERVICE CATEGORIES - IAAS

On-premises	IaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

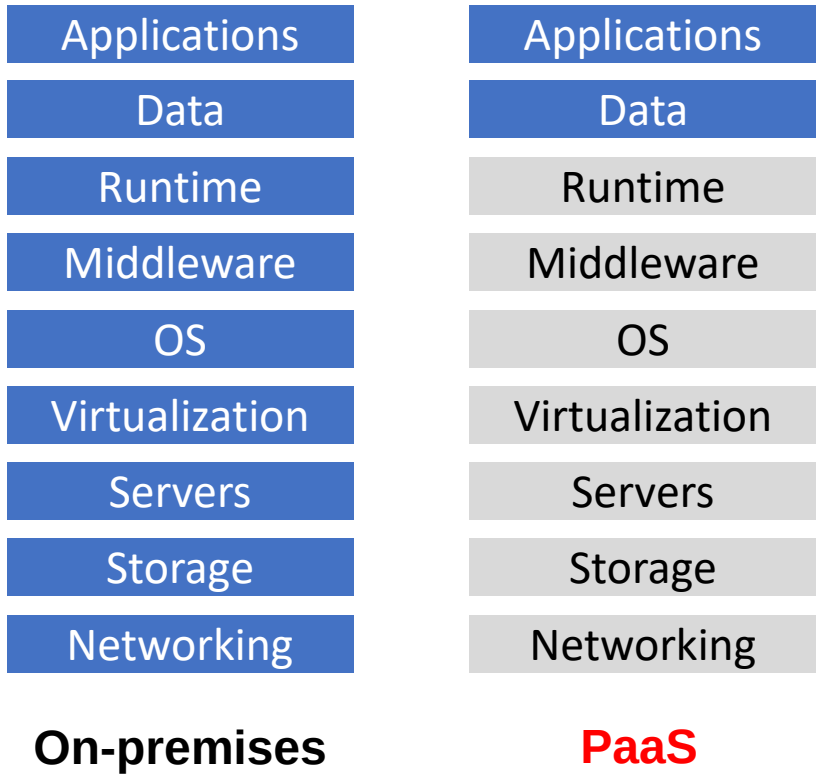
Azure Virtual Machines

Amazon EC2



GCP Compute Engine

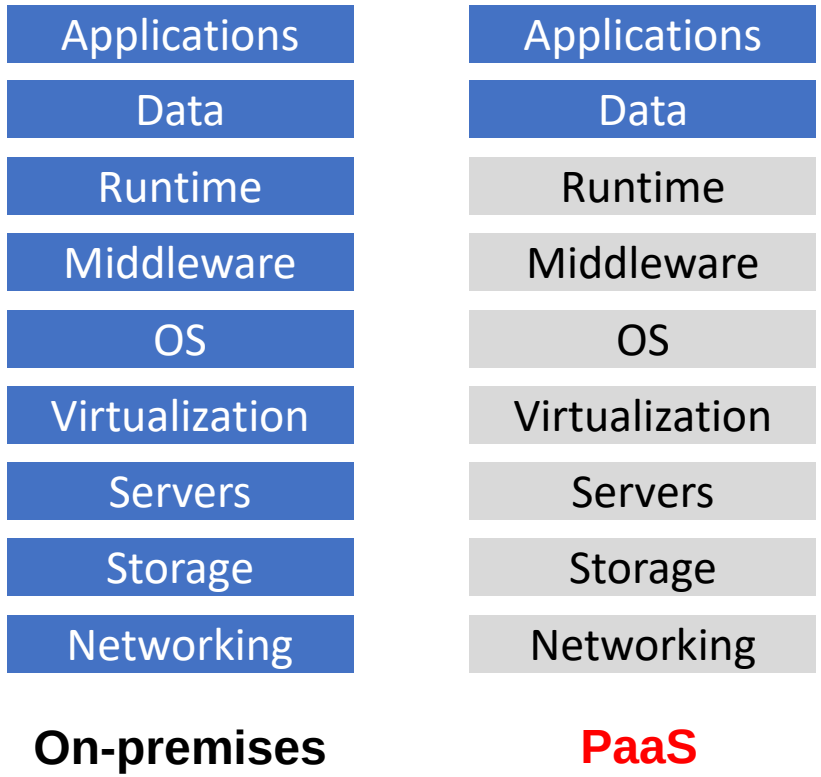
CLOUD SERVICE CATEGORIES - PAAS



Customer is responsible for deployment and management of apps

CSP manages provisioning, configuration, hardware, and OS

CLOUD SERVICE CATEGORIES - PAAS



Key Benefits

Core infrastructure updated by provider

Global collaboration for app development

Running multiple languages seamlessly

CLOUD SERVICE CATEGORIES - PAAS

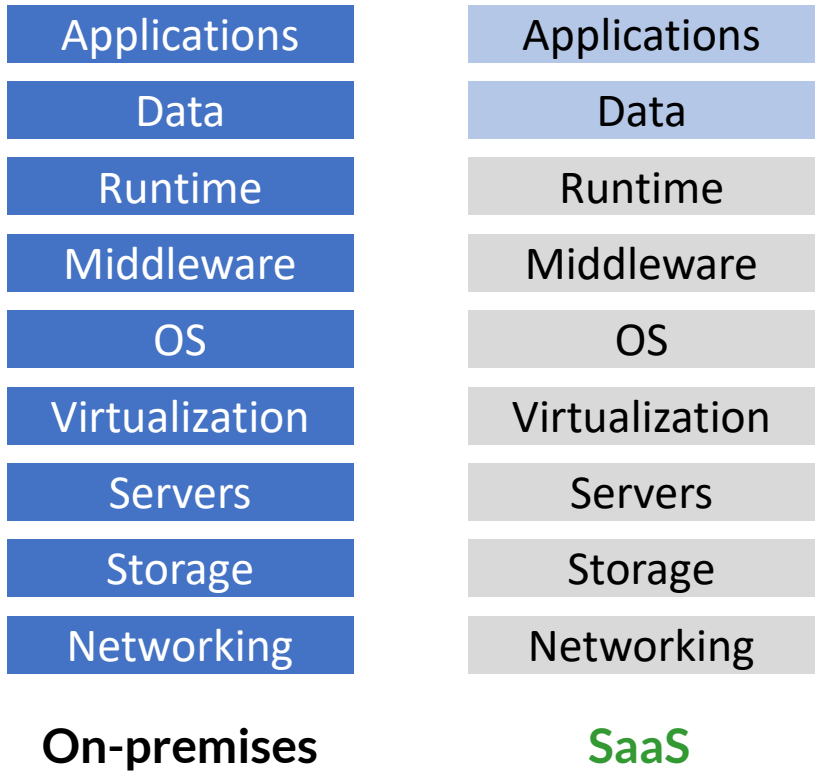
On-premises	PaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

Azure SQL Database

API Management

Azure App Service

CLOUD SERVICE CATEGORIES - SAAS

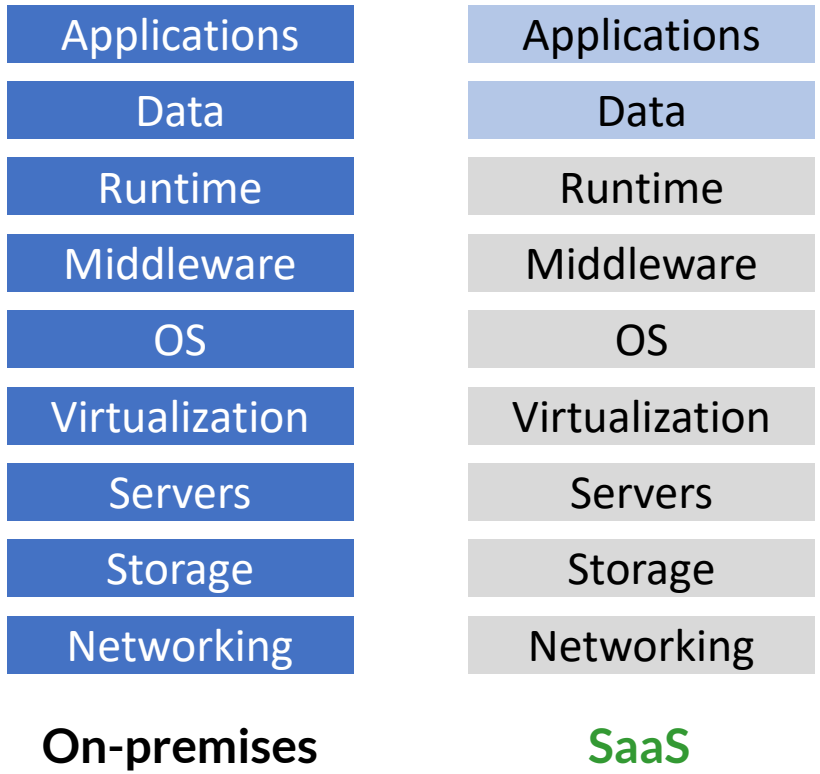


Customer has some responsibility in access management and data recovery

Customer just **configures features**.

CSP is responsible for management, operation, and service availability.

CLOUD SERVICE CATEGORIES - SAAS



Key Benefits

Limited administration responsibility

Limited skills required

Service always up-to-date

Global access

CLOUD SERVICE CATEGORIES - SAAS

On-premises	SaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

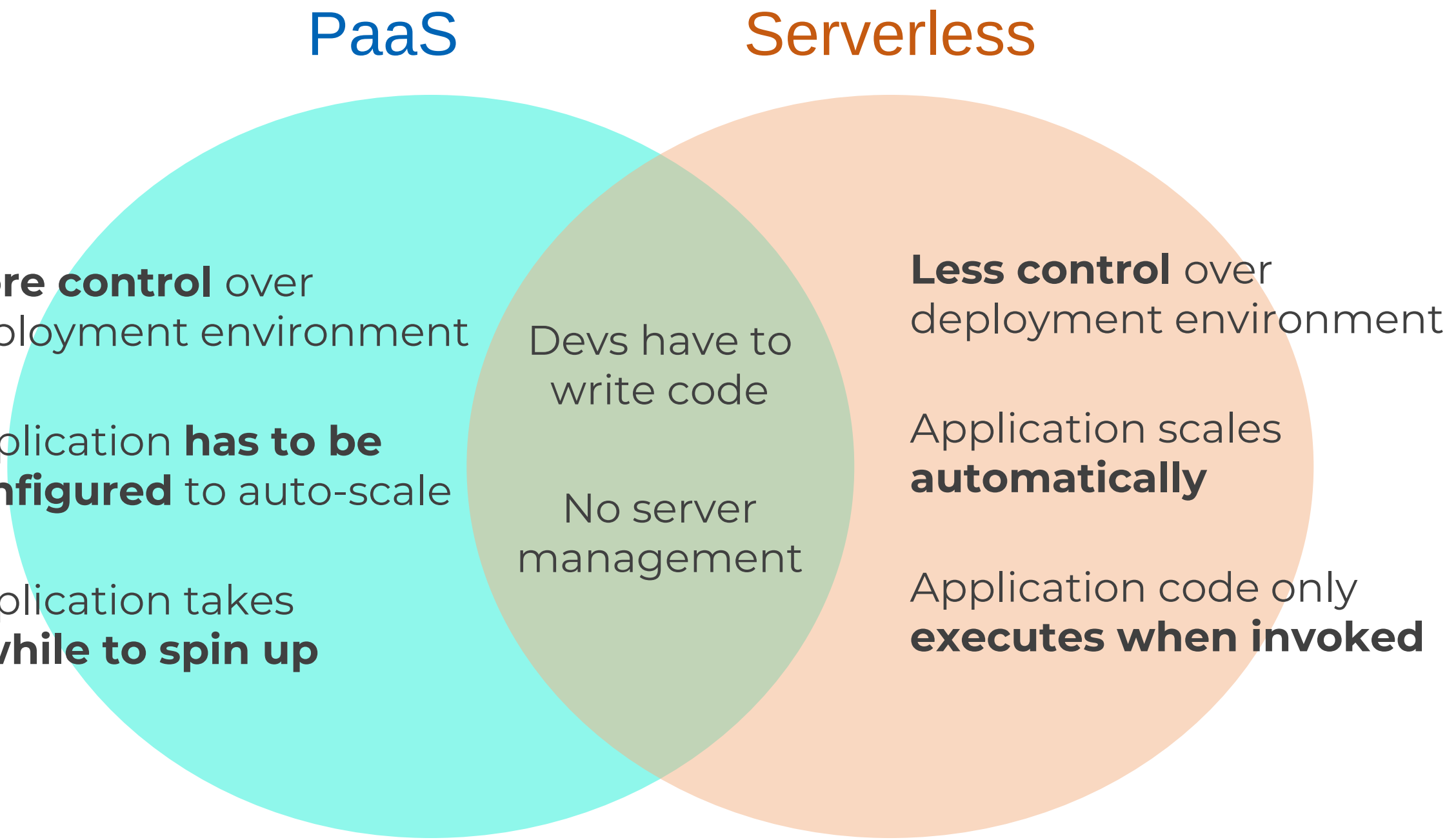
HOW

is SERVERLESS

DIFFERENT

from PAAS in terms of

RESPONSIBILITY?


PaaS
Serverless
More control over deployment environment
Application has to be configured to auto-scale
Application takes a while to spin up
Devs have to write code
No server management
Less control over deployment environment
Application scales automatically
Application code only executes when invoked

CLOUD COMPUTING CONCEPTS

Serverless Architecture

a cloud computing execution model where the cloud provider dynamically manages the allocation and provisioning of servers.

hosted as a pay-as-you-go model based on use.

Resources are stateless, servers ephemeral and often capable of being triggered

Example:
Function-as-service

Services Integration

Provisioning of **multiple business services** is combined with different **IT services** to provide a single business solution.

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Benefits of Cloud Computing

Cloud is **cost-effective**, **global**, **secure**, **scalable**, **elastic**, and **always current**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Public Cloud

Everything runs on your
cloud provider's hardware.

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Public Cloud

Advantages include **scalability**, **agility**, **PAYG**, no **maintenance**, and **low skills**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

A cloud environment **in your own datacenter**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

A cloud environment **dedicated to a single customer**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

Advantages include **legacy support**, **control**, and **compliance**

Enables greater control of upgrade cycles in legacy apps and some compliance scenarios

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Hybrid Cloud

Combines public and private clouds, allowing you to run your apps in the right location

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Hybrid Cloud

Advantages include **flexibility** in legacy, compliance, and scalability scenarios

Enables the organization to control the pace of public cloud adoption

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Community Cloud

Similar to private clouds in that they are **not open the general public**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Community Cloud

But they are **shared by several related organizations** in a common community

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Multi-Cloud

Combines resources from **two or more public cloud providers**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Multi-Cloud

Allows orgs to take advantage of service and price differences, but at the cost of **added complexity**

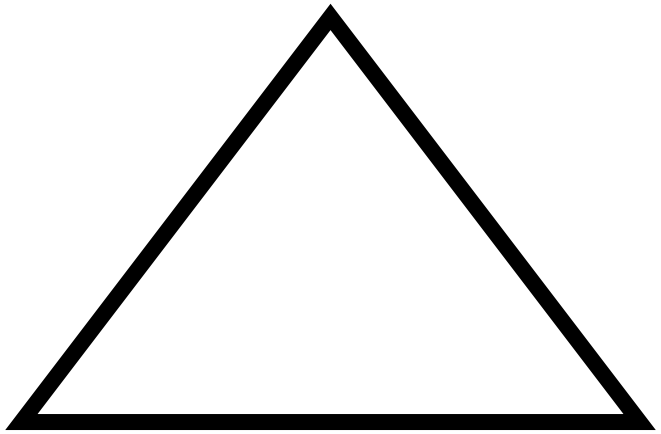
Confidentiality

Integrity

Availability

1

Confidentiality

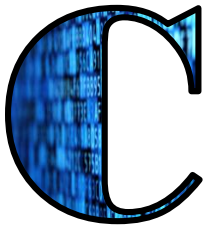


2

Integrity

3

Availability

 onfidentiality

Access controls help ensure that only authorized subjects can access objects

 ntegrity

Ensures that data or system configurations are not modified without authorization

 vailability

Authorized requests for objects must be granted to subjects within a reasonable amount of time

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Interoperability

3rd parties, other CSPs

Ability of one cloud service to interact with other cloud services by exchanging information according to a prescribed method and obtain predictable results.

Most CSPs have a cloud marketplace with certified apps and services

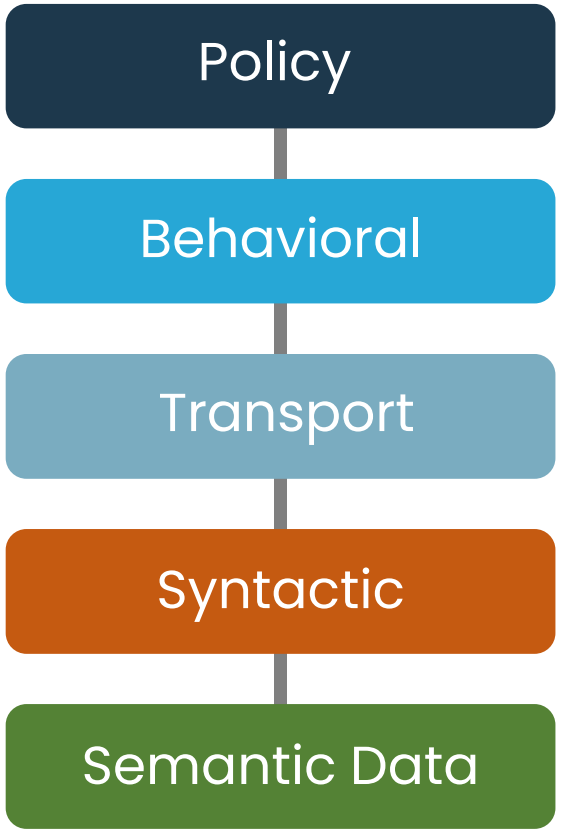
Reversibility

Process for cloud service customers to retrieve their data and application artifacts **AND**

for the CSP to delete all cloud service customer data and contractually specified cloud service derived data after an agreed period.

Customer access to data also appears in regulations (e.g. GDPR)

5 FACETS OF CLOUD INTEROPERABILITY



The five facets of **cloud interoperability** are:

Policy. Ability of two or more systems to interoperate while complying with governmental laws, regulations, and organizational mandates

Behavioral. Where the results of the use of the exchanged information matches the expected outcome

Transport. The commonality of the communication between cloud consumer and provider and other providers (e.g., HTTP/S, and various message queuing standards)

Syntactic. Two or more systems to understand the other systems' structure of exchanged information through encoding syntaxes (e.g., JSON and XML)

Semantic data. Ability of systems exchanging information to understand the meaning of the data model within the context (e.g., virtual machines, containers, storage, and networking concepts)

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Portability

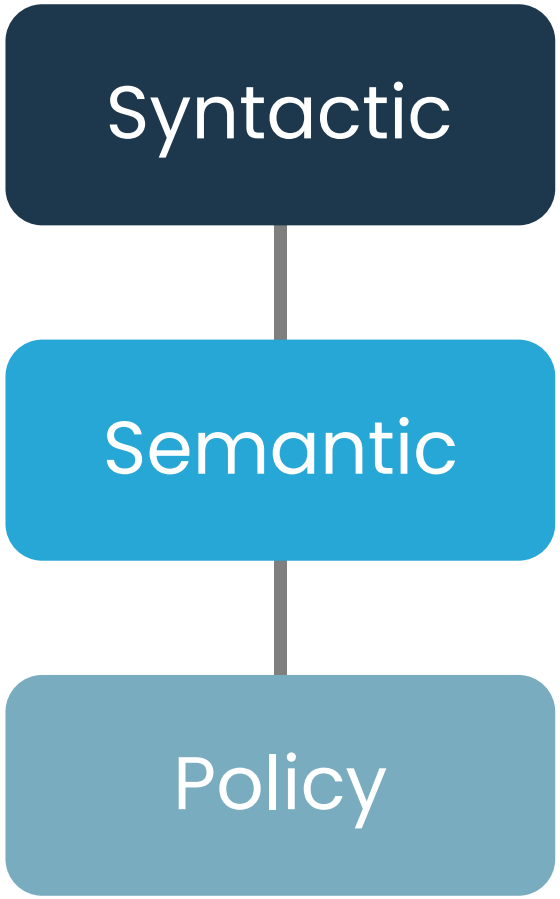
Ability to move applications and associated data between cloud providers (CSPs), between legacy and cloud environments, or between public and private cloud environments. ← Hybrid cloud

Cloud data portability is the ability to easily move data from one cloud service to another without the need to re-enter the data.

Cloud application portability is the ability to migrate an application from one CSP to another or between a customer's environment and a cloud service.

Portability prevents "vendor lock-in"

3 FACETS OF CLOUD DATA PORTABILITY



The three facets of **cloud data portability** are:

1. Syntactic

Transferring data from a source system to a target system using formats that can be decoded on the target system with features like XML or Open Virtualization Format (OVF)

2. Semantic

Transferring data from a source system to a target system so that the data model is understood within the context of the subject area by the target

3. Policy

Transferring data from a source system to a target system so that governmental laws, regulations, and organizational mandates are followed

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Availability

We'll discuss SLAs, OLAs, and PLAs in depth in Domain 6

Systems and resource availability defines the success or failure of a cloud-based service.

Check service-level SLAs and how multi-service SLAs are calculated.

Resiliency

ability of a cloud services data center and its associated components, including servers, storage, and so on, to continue operating in the event of a disruption.

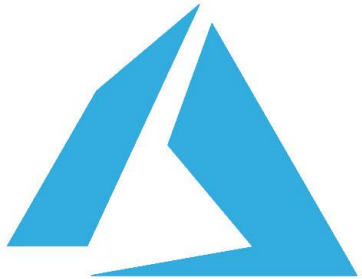
Look for a cloud provider with **global presence**, **regional redundancy** and **zone redundancy** within region.

The following example explains these concepts in Microsoft Azure.

AWS and GCP support the same concepts

The CCSP exam is CSP-agnostic

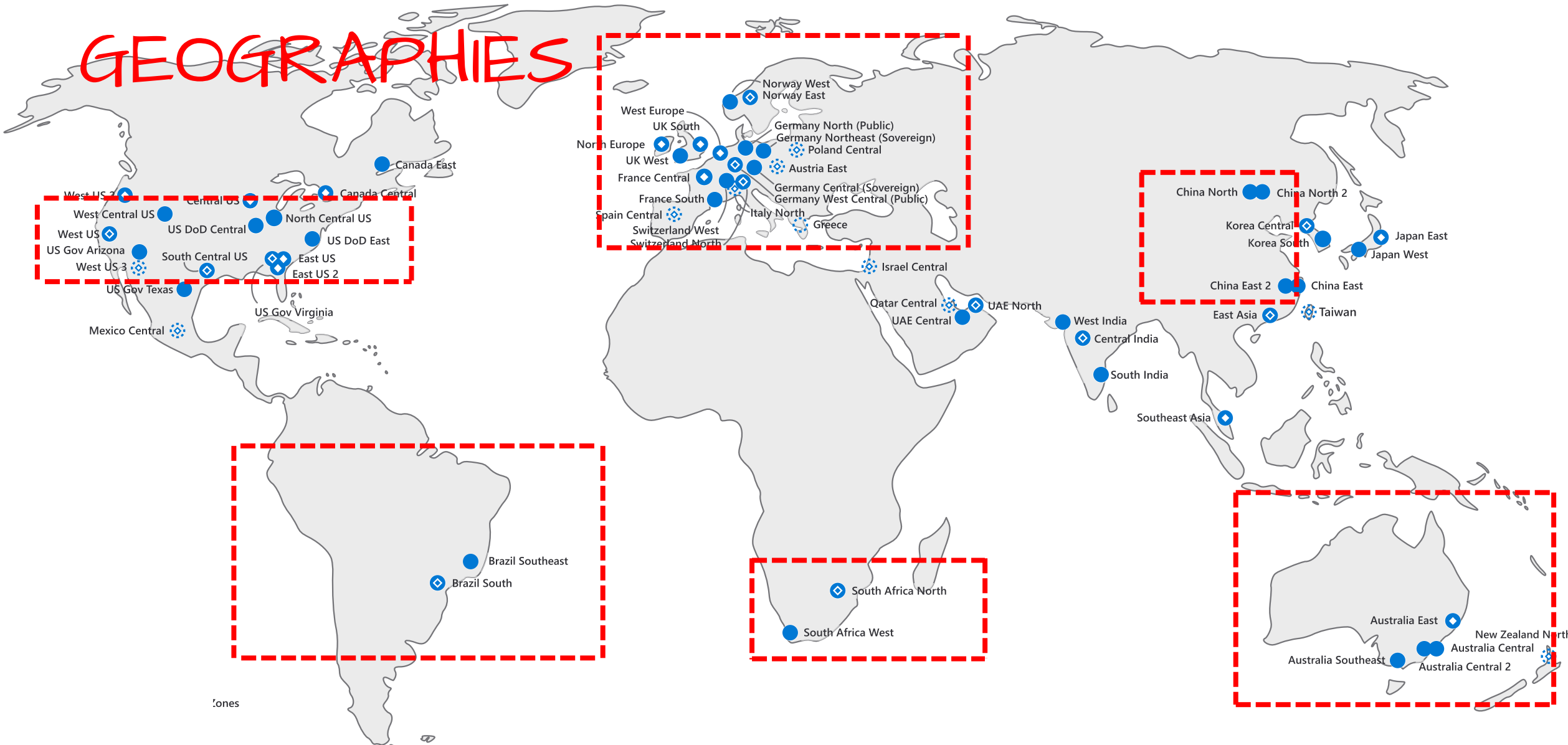
DESCRIBE CORE ARCHITECTURE COMPONENTS



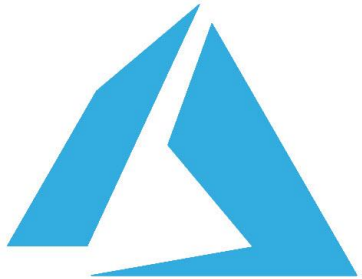
Azure Geography

A **discrete market**, typically containing two or more regions, that preserves data residency and compliance boundaries

DESCRIBE CORE ARCHITECTURE COMPONENTS



DESCRIBE CORE ARCHITECTURE COMPONENTS



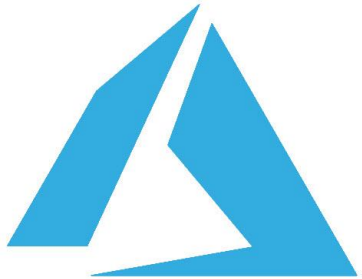
Azure Regions

A **set of datacenters** deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

DESCRIBE CORE ARCHITECTURE COMPONENTS

REGIONS

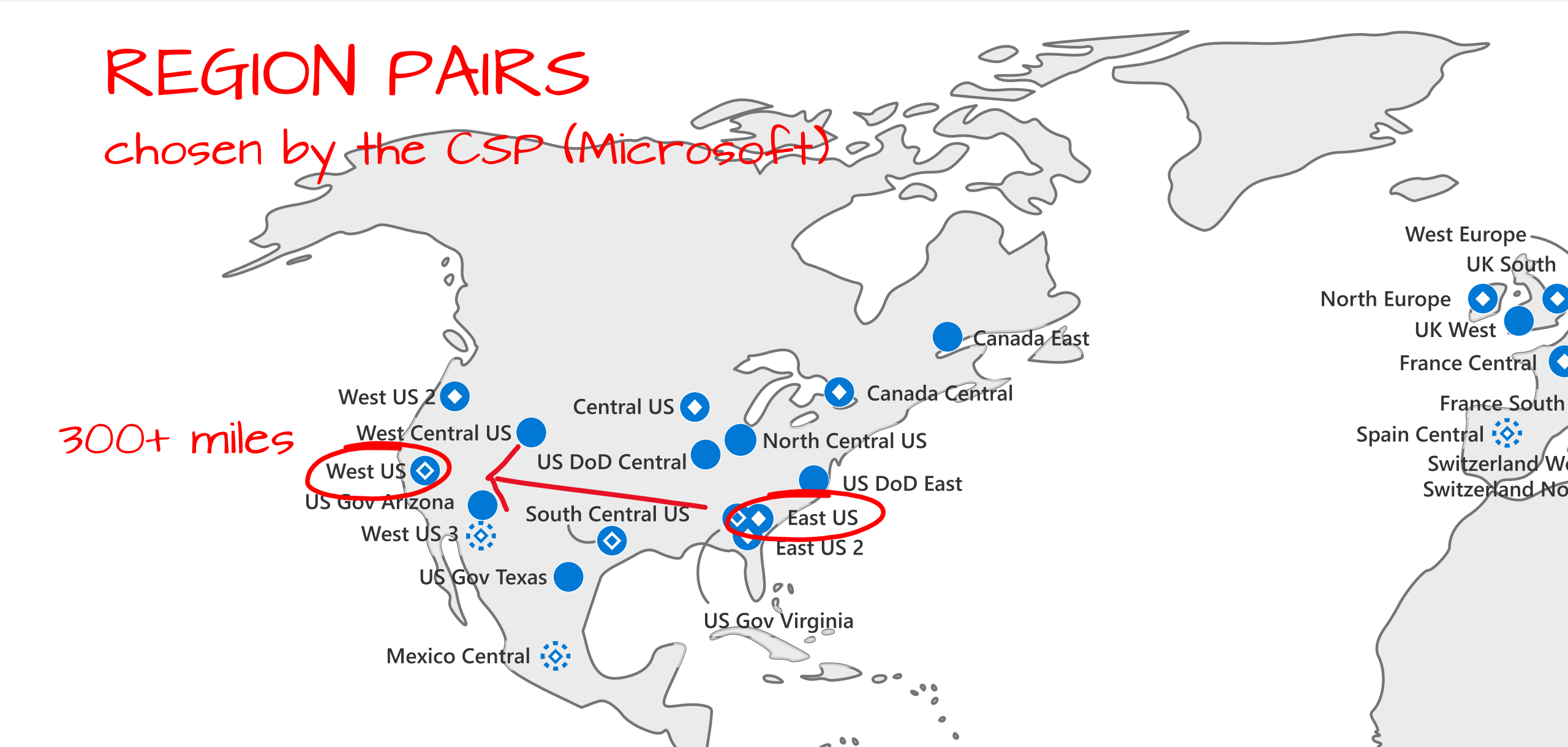
DESCRIBE CORE ARCHITECTURE COMPONENTS



Region Pairs

A relationship between **2 Azure Regions** within the same geographic region for disaster recovery purposes.

DESCRIBE CORE ARCHITECTURE COMPONENTS



DESCRIBE CORE ARCHITECTURE COMPONENTS

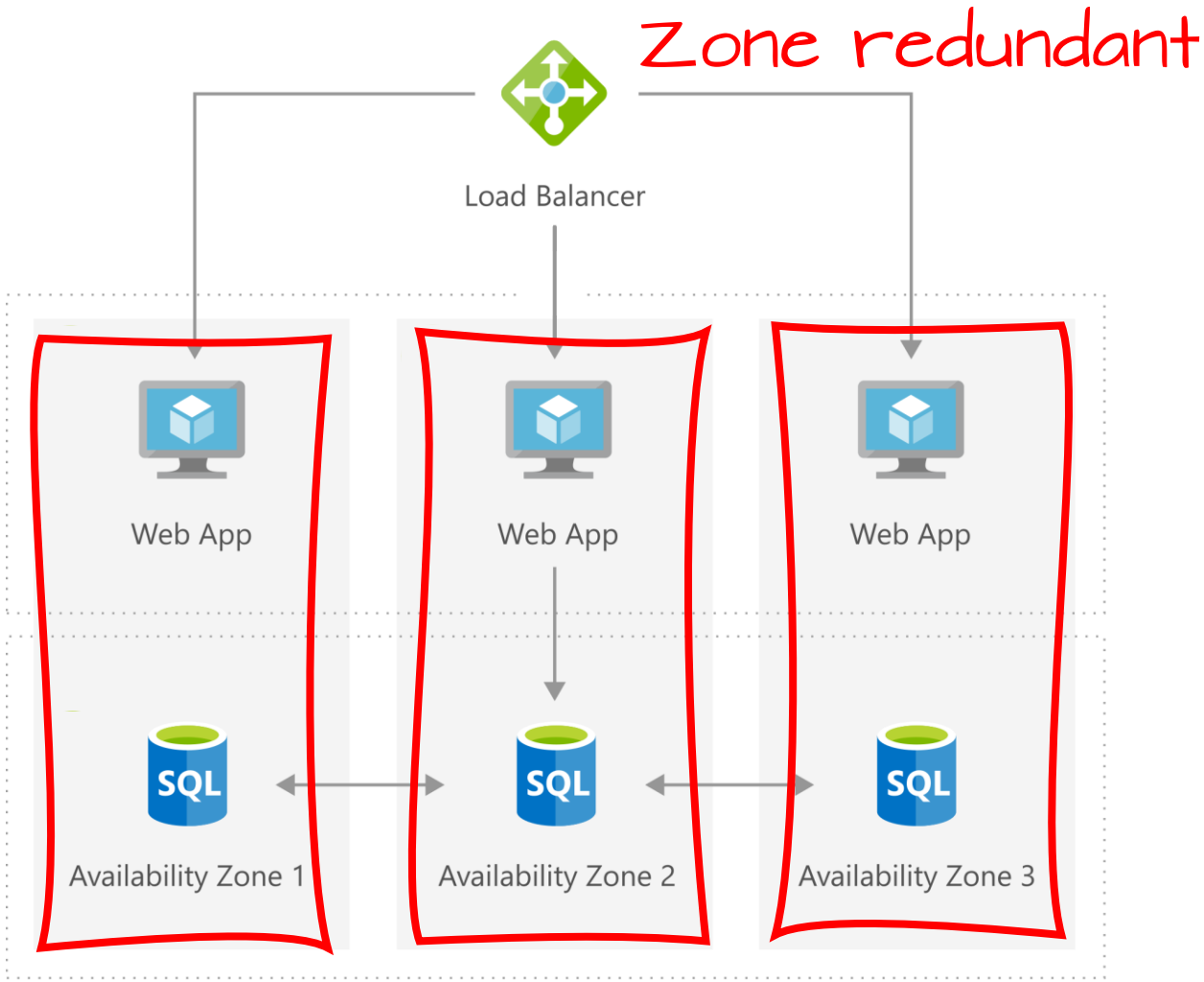
Availability Zones

Unique physical locations within a region with independent power, network, and cooling

Comprised of one or more datacenters

Tolerant to datacenter failures via redundancy and isolation

FOCUS: datacenter failures within a region



CLOUD SHARED CONSIDERATIONS

Security

Protection of customer **data** (access control, encryption)

Protection of cloud **applications**

Protection of cloud **infrastructure**

The **Shared Responsibility Model** explains who is responsible for security in each model and scenario.

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Privacy

Data privacy in cloud computing allows collecting, storing, transferring and sharing the data over the cloud network without putting the privacy of personal data at risk.

Prominent sources of privacy concerns

Many times, customer does not have knowledge about how their personal information is stored and processed in the cloud.

Data breaches have brought data privacy to the forefront as a crucial factor in cloud computing.

Privacy vs Confidentiality

What is the difference?

Privacy

The right of an individual to have some control over how their personal information (PII,PHI) is collected, used, and potentially disclosed.

Focus on rights of the individual person/customer

Confidentiality

The duty to ensure private information is kept secret to the extent possible.

A legal obligation in regulatory scenarios, and a due care obligation in U.S. law

Focuses on data

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Performance

Ability of a service to remain responsive to requests to that service with an acceptable level of response latency or processing time.

Public cloud delivers the perception of unlimited scale for than for less than the cost a customer would incur in their own datacenter.

Governance

Enforcement of security policies and regulatory requirements, often through policy controls and regular audits.

CSPs often have policy automation in which restrictions can be defined and automatically enforced throughout the service lifecycle.

CLOUD SHARED CONSIDERATIONS

Considerations in a shared (multitenant) environment

Auditability

Ability to provide clear documentation of the actions in a data event. (e.g. data breach, unauthorized access)

Related activities

Accountability. Ability to determine who caused the event. This is known sometimes called "identity attribution". Requires non-repudiation

Traceability. Ability to track down all events related to the investigated event.

Auditability is only possible with proper logging providing accountability and traceability !

SERVICE-LEVEL AGREEMENTS (SLA)

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Generally used with vendors

SERVICE-LEVEL AGREEMENTS (SLA)

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Operating Level Agreements (OLAs) and Privacy Level Agreements (PLAs) may also appear on the exam (Domain 6)

OUTSOURCING

Obtaining goods or a services, such as cloud services from an external supplier.

Introduces considerations including **reversibility**, **interoperability**, and **vendor lock-in**.

Vendor lock-in is a technical or contractual constraint that prevents a customer from moving from a provider.

IMPACT OF RELATED TECHNOLOGIES

Core (mentioned in syllabus)

- ✓ Data science
- ✓ Machine learning
- ✓ Artificial intelligence
- ✓ Blockchain
- ✓ DevSecOps
- ✓ Internet of Things (IoT)
- ✓ Containers
- ✓ Quantum computing
- ✓ Confidential Computing
- ✓ Edge computing

Extras (related or mentioned in OSG)

- ✓ Deep Learning
- ✓ Fog Computing
- ✓ Post-Quantum Cryptography

DATA SCIENCE

The study of data to extract meaningful insights for business

Combines principles and practices from multiple fields (mathematics, artificial intelligence, computer engineering) to analyze large amounts of data.

Helps data scientists to ask and answer questions about past, current, and future events through evaluation of data.

Cybersecurity Data Science (CSDS)

The practice of applying data science to prevent, detect, and remediate cybersecurity threats.

Data is collected from selected cyber security sources and then analyzed to provide timely, data-driven patterns at scale.

GOAL: deliver more effective security insights at scale

ARTIFICIAL INTELLIGENCE vs MACHINE LEARNING

Knowing the difference will help on the exam!

Artificial Intelligence

Focuses on accomplishing "smart" tasks combining machine learning and deep learning to emulate human intelligence

Machine Learning

A subset of AI, computer algorithms that improve automatically through experience and the use of data.

Deep Learning

a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called **artificial neural networks**.

BLOCKCHAIN

Blockchain was originally the technology that powered Bitcoin but has broader uses.

A **distributed, public ledger** that can be used to store financial, medical, or other transactions. Anyone is free to join and participate

Does not use intermediaries such as banks and financial institutions.

Data is "chained together" with a block of data holding both the hash for that block and the hash of the preceding block.

To create a new block on the chain, the computer that wishes to add the block solves a cryptographic puzzle and sends the solution to the other computers participating in that blockchain.

This is known as "proof of work"

IMPACT OF RELATED TECHNOLOGIES

Internet of Things

A class of devices connected to the internet in order to provide automation, remote control, or AI processing in a home or business setting

questions involving IoT devices are more likely to appear in 2022 exam update

INTERNET OF THINGS

Default settings in business scenarios, lingers due to a process issue

Every device that you put on your network to manage has a default username and a default password.

Often, the defaults are open and available for anybody to use. (wi-fi and IoT)

Botnets and offensive security tools will find, and exploit devices with weak default settings still in place. Simply change defaults to shut down this attack vector!

Wearables.

You might be wearing an IoT device, such as a fitness tracker or smartwatch.

Facility automation.

In a large facility, IoT devices able to manage the heating and AC, lights, and motion/fire/water detection.

Enable facility managers to be able to configure automation and monitoring of device function.

Sensors.

Vehicles have very specialized sensors embedded, assisting with vehicle function

Containerization

Examples include Docker and Kubernetes

A lightweight, granular, and portable way to package applications for multiple platforms.

Reduces overhead of server virtualization by enabling containerized apps to run on a shared OS kernel.

containers do not have their own OS !

Share many concerns of server virtualization: isolation at host, process, network, and storage levels

Can be used in some cases to isolate existing applications developed to run in a VM with a dedicated operating system.

Quantum Computing

A rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

Replaces the binary one and zero bits of digital computing with multidimensional quantum bits known as qubits.

No widespread use cases as of 2023, so little impact outside the world of scientific research and testing.

This is where 'post-quantum cryptography' can help!

A quantum computer could render all modern cryptography completely ineffective and require the redesign of new, stronger quantum encryption algorithms.

DOMAIN 1: QUANTUM COMPUTING

Quantum cryptography

the practice of harnessing the principles of quantum mechanics to improve security and to detect whether a third party is eavesdropping on communications.

Leverages fundamental laws of physics such as the observer effect, which states that it is impossible to identify the location of a particle without changing that particle.

Quantum Key Distribution

is the most common example of quantum cryptography.

by transferring data using photons of light instead of bits, a confidential key transferred between two parties cannot be copied or intercepted secretly.

Post-quantum cryptography

Post-quantum cryptography refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer.

Post-quantum cryptography focuses on preparing for the era of quantum computing by updating existing mathematical-based algorithms and standards.

What is **post-quantum cryptography**?

The development of new kinds of cryptographic approaches that can be implemented using today's conventional computers.

...but will be impervious (resistant) to attacks from tomorrow's quantum computers.

POST-QUANTUM CRYPTOGRAPHY

What is **post-quantum cryptography**?

The development of new kinds of cryptographic approaches that can be implemented using today's conventional computers.

...but will be impervious (resistant) to attacks from tomorrow's quantum computers.

Post-quantum algorithms are sometimes called "quantum-resistant" cryptographic algorithms

Edge Computing

Some compute operations require processing activities to occur locally, far from the cloud.

Common in various Internet-of-things scenarios, like agricultural, science/space, military.

All the processing of data storage is closer to the sensors rather than in the cloud data center.

With large network-connected device counts in varied locations, **data encryption**, **spoofing protection**, and **authentication** are key

Fog Computing

Complements cloud computing by processing data from IoT devices.

Often places gateway devices in the field to collect and correlate data centrally at the edge.

Generally, brings cloud computing nearer to the sensor to process data closer to the device.

Important to **speed processing time** and **reduce dependence** on cloud/Internet connectivity mission critical situations (healthcare)

Confidential Computing

PROBLEM: Sensitive data must be encrypted in memory before an app can process it, leaving the data vulnerable

Confidential computing solves for this by isolating sensitive data in a protected CPU enclave during processing.

This CPU enclave is called a trusted execution environment (TEE), secured with embedded encryption keys.

Embedded attestation mechanisms ensure that the keys are accessible only to authorized application code.

DevSecOps

A portmanteau development, security, and operations.

Integrates security as a shared responsibility throughout the entire IT lifecycle.

Builds a security foundation into DevOps initiatives.

Often includes automating some of the security gates in the DevOps process.

INFRASTRUCTURE AS CODE

IaC

Infrastructure as Code

is the management of cloud infrastructure (networks, VMs, load balancers, and connection topology) described in code

just as the same source code generates the same binary, code in the IaC model results in the same environment every time it is applied.

IaC is a key DevOps practice and is used in conjunction with **C**ontinuous **I**ntegration and **C**ontinuous **D**elivery (CI/CD). "the CI/CD pipeline"

IaC, **CI/CD**, and **DevOps** are standard elements of deployment, change, and release in the cloud. **DevSecOps** is quickly growing in popularity.

1. CLOUD CONCEPTS, ARCHITECTURE, AND DESIGN

1.3 Understand Security Concepts Relevant to Cloud Computing

Cryptography and Key Management

Identity and Access Control
(e.g., user access, privilege access, service access)

Data and Media Sanitization
(e.g., overwriting, cryptographic erase)

Network Security
(e.g., network security groups, traffic inspection, geofencing, zero trust network)

Virtualization Security
(e.g., hypervisor security, container security, ephemeral computing, serverless technology)

Common Threats

Security hygiene
(e.g., patching, baselining)

Trusted Platform Module

A chip that resides on the motherboard of the device.

Multi-purpose, like storage and management of keys used for full disk encryption (FDE) solutions.

Provides the operating system with access to keys, but prevents drive removal and data access

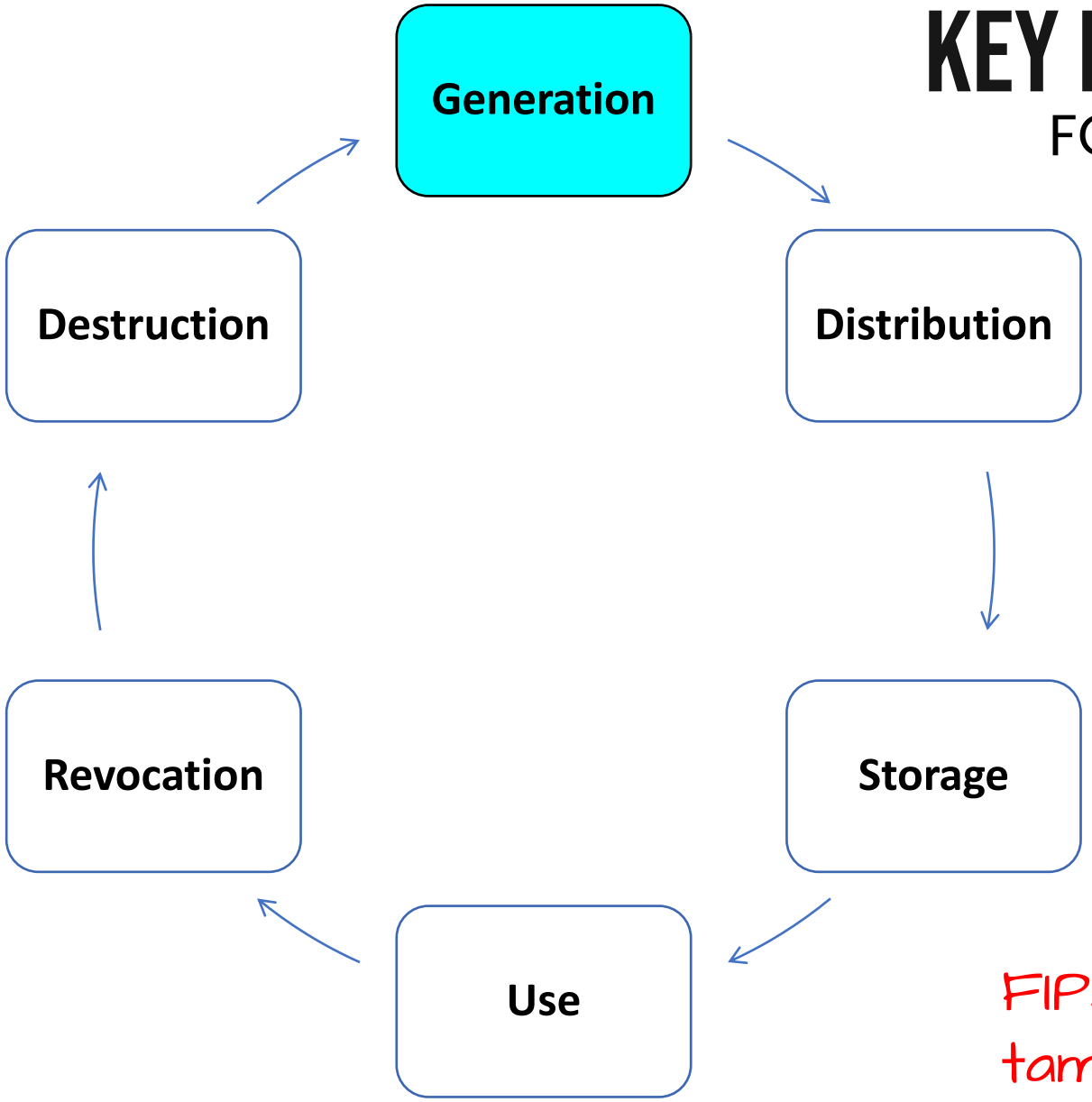
Hardware Security Module (HSM)

a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

Like a TPM, but are often removable or external devices

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE

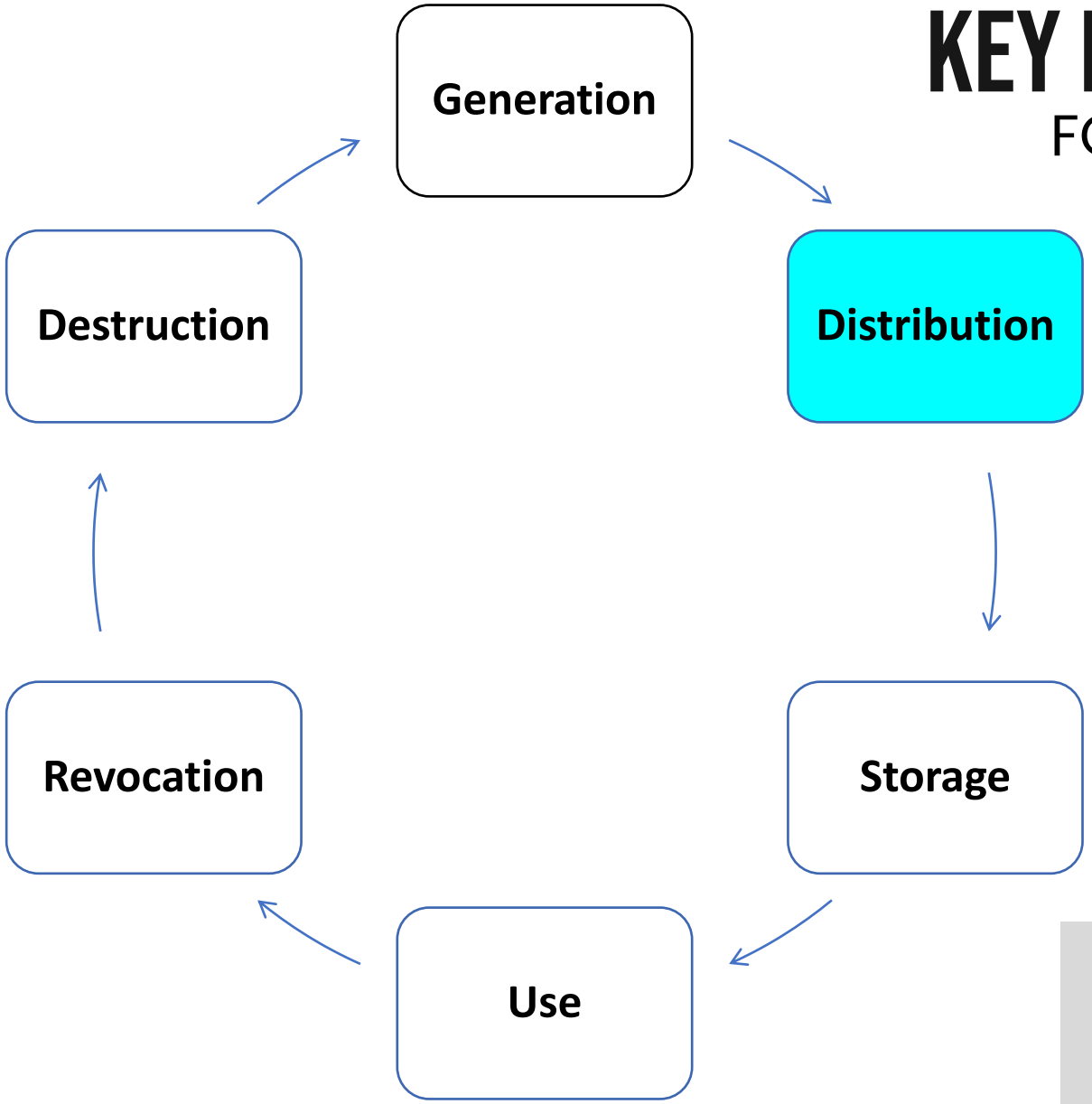


Encryption keys should be generated within a trusted, secure cryptographic module

FIPS 140-2 validated modules provide tamper resistance and key integrity

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



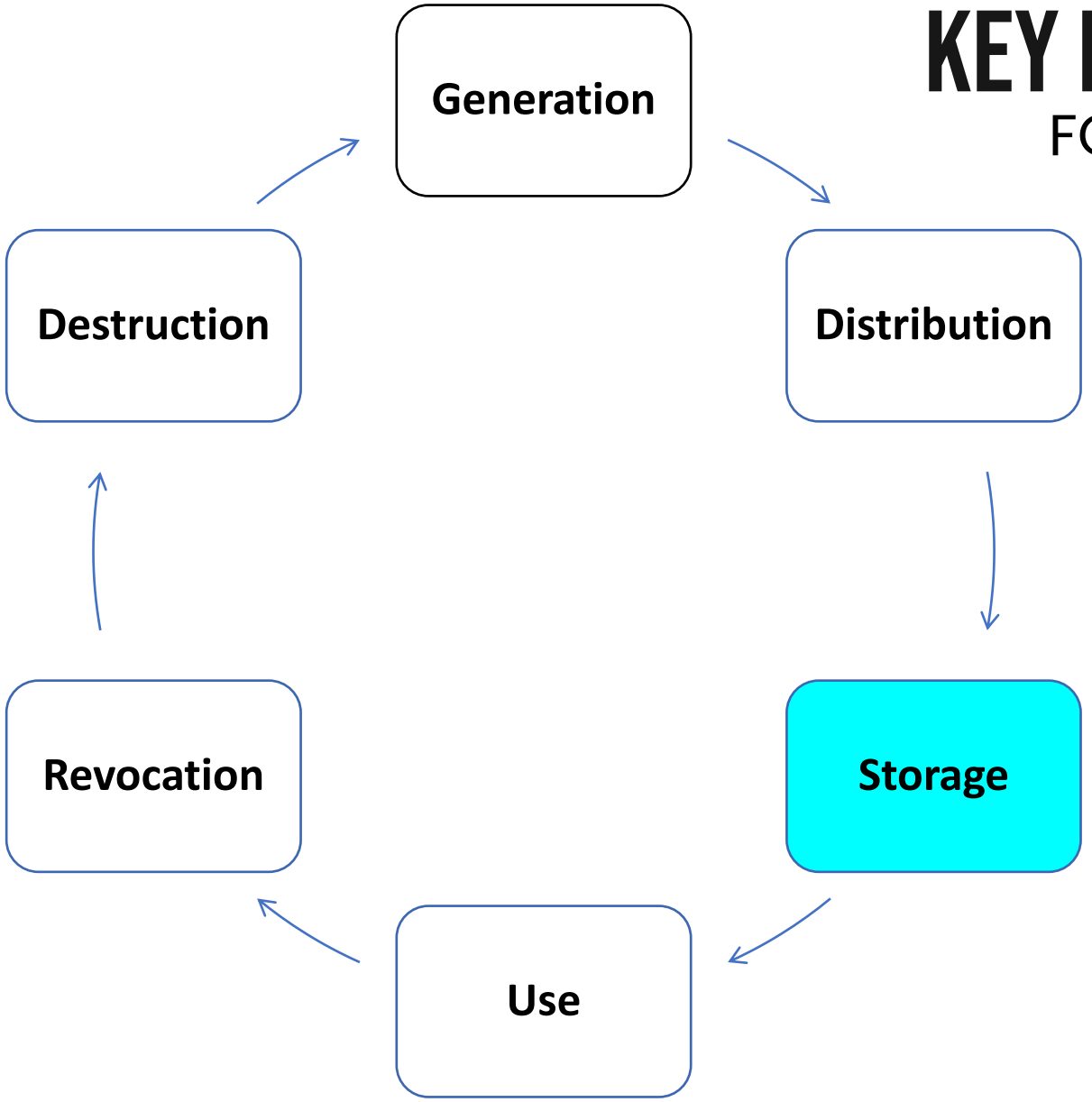
Encryption keys should be distributed securely to prevent theft/compromise during transit

BEST PRACTICE:

Encrypt keys with a separate encryption key while distributing to other parties

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE

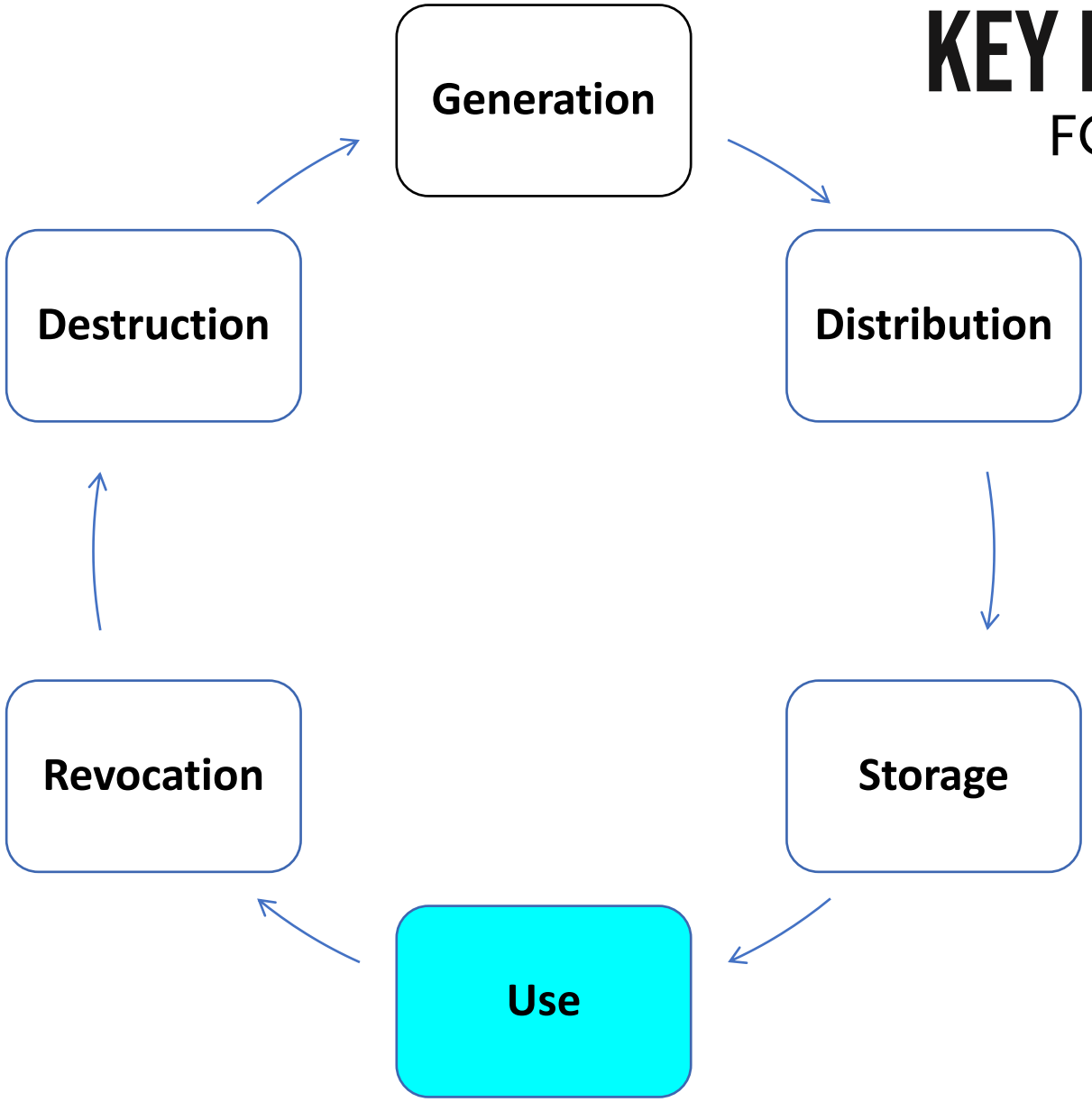


Encryption keys must be protected at rest and should never be stored in plaintext

This includes keys in volatile and persistent memory

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE

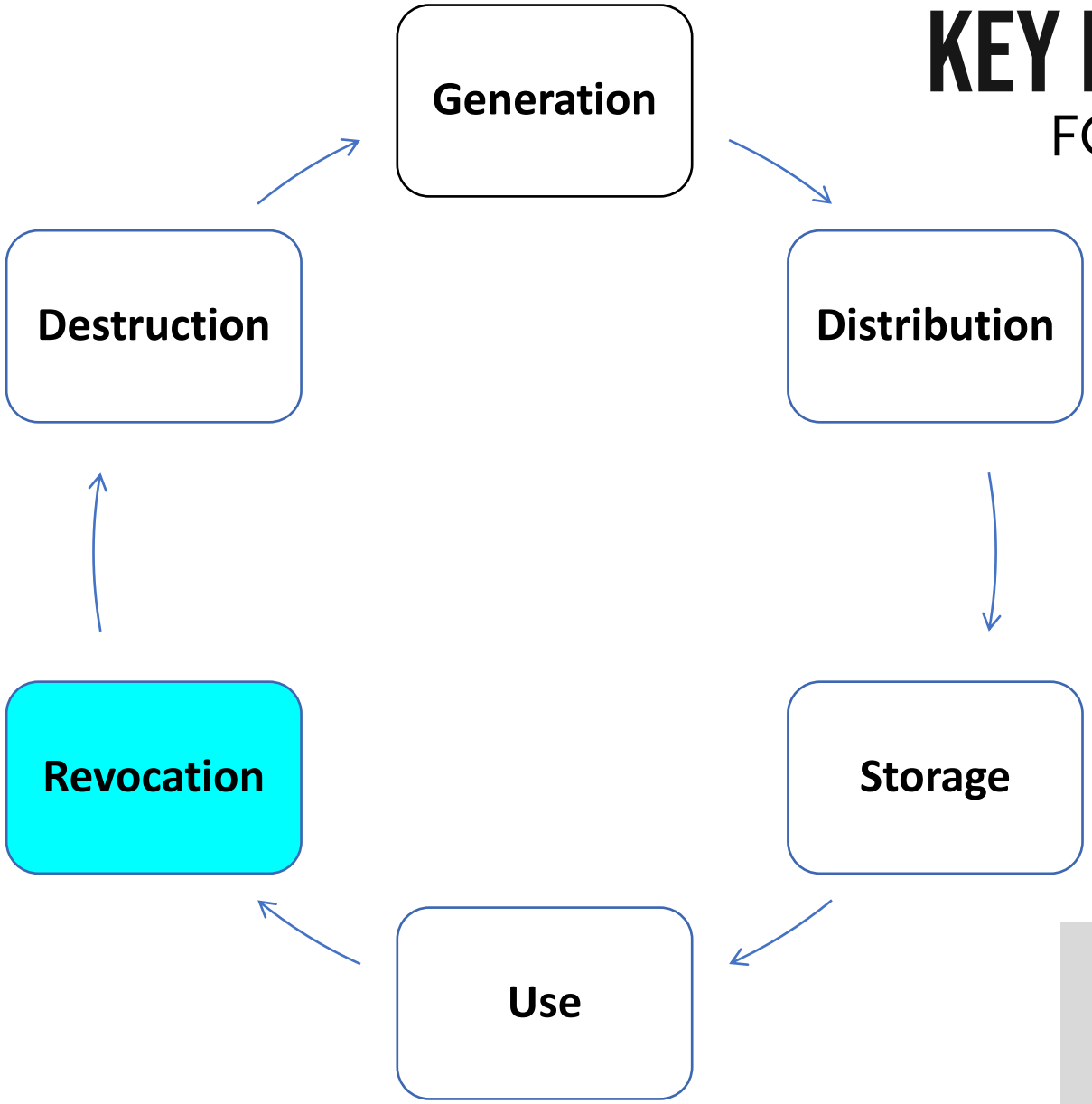


Clients (users + trusted devices) will use keys for resource access as access controls allow.

Acceptable use policy sets guardrails for data usage

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



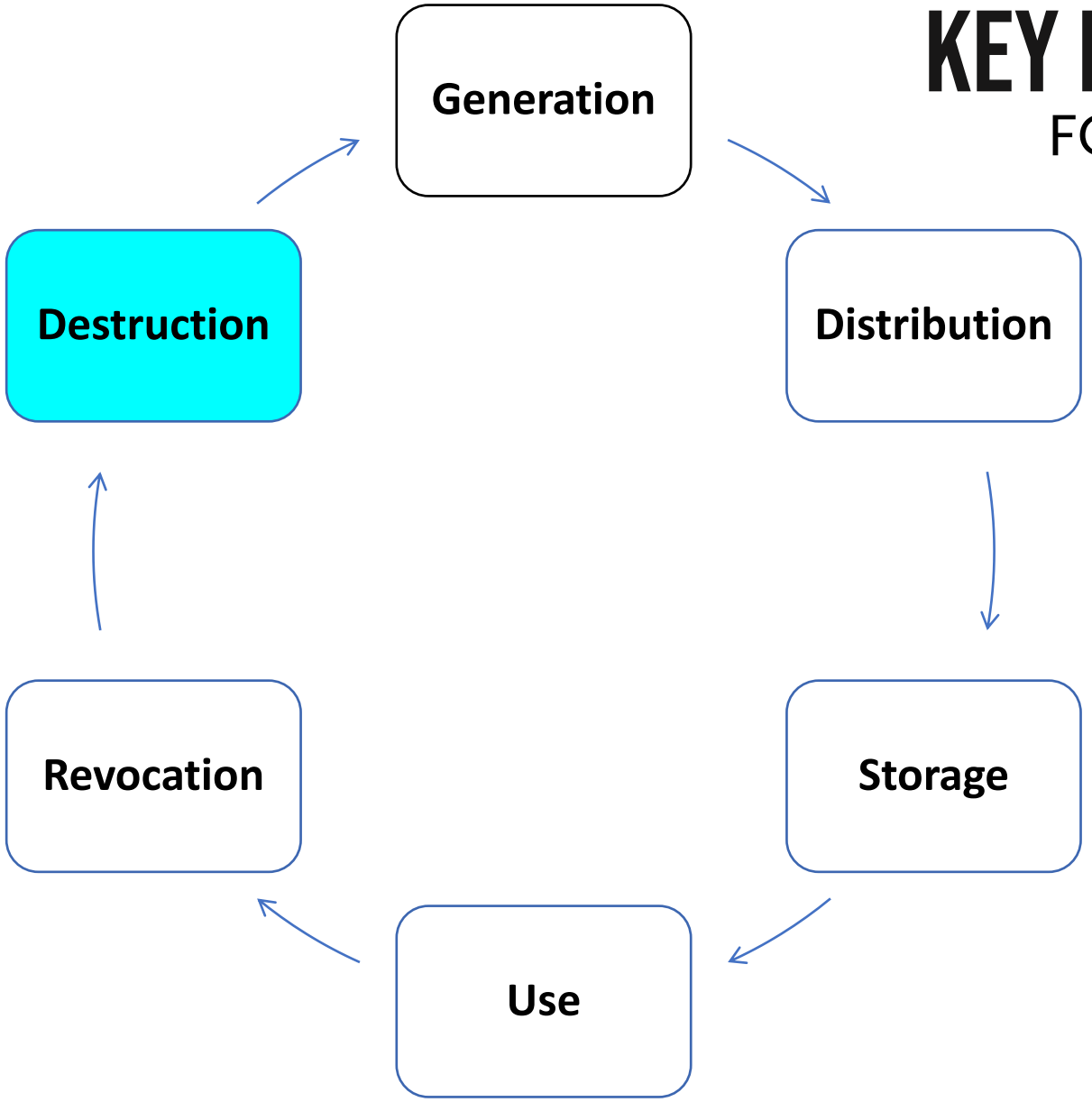
A process for revoking access at separation, policy breach, device or key compromise.

EXAMPLE:

In PKI, you would revoke the certificate on the issuing Certificate Authority (CA)

KEY MANAGEMENT STRATEGY

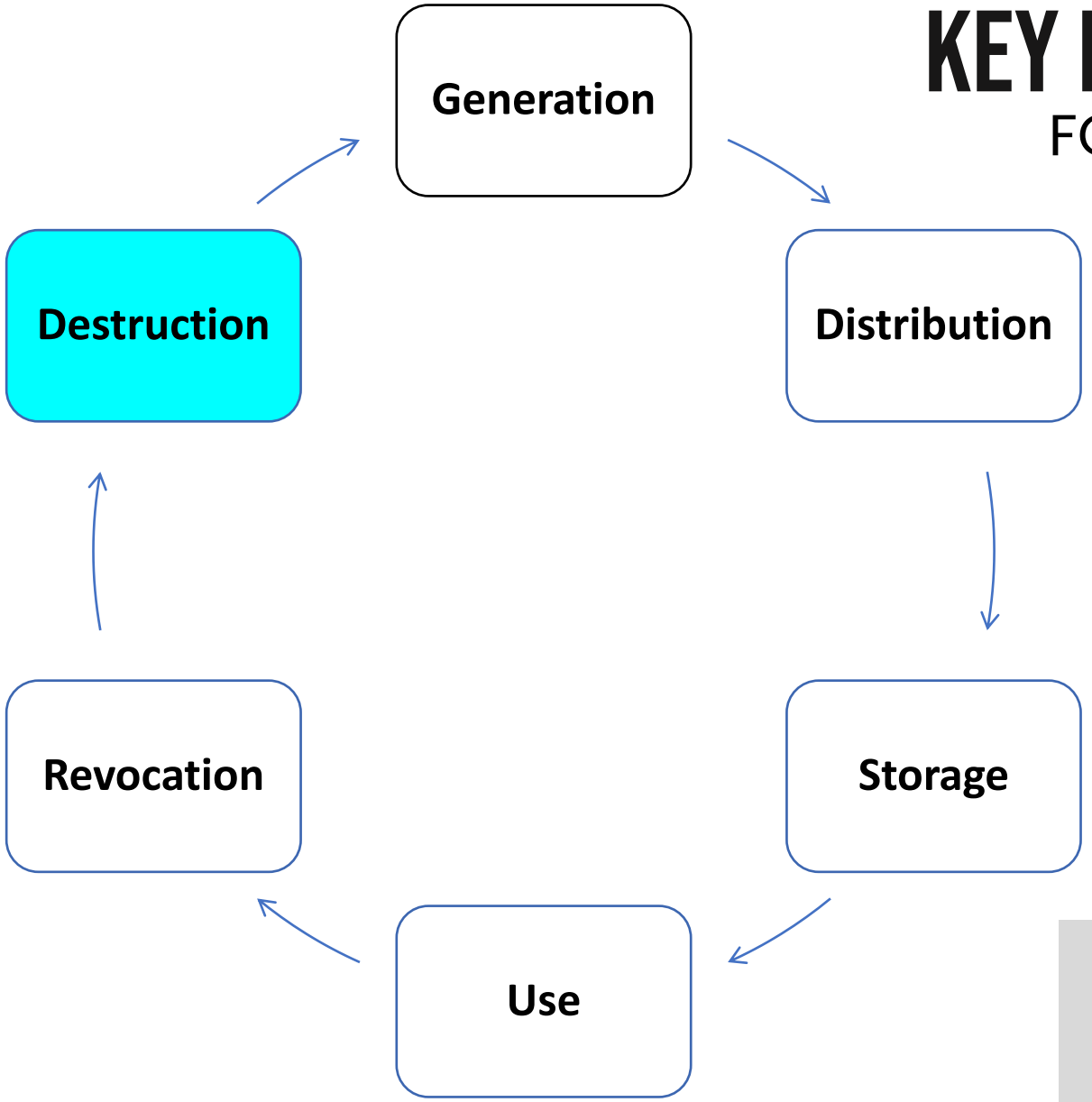
FOR ENCRYPTION KEY LIFECYCLE



Key destruction is the removal of an encryption key from its operational location.

KEY MANAGEMENT STRATEGY

FOR ENCRYPTION KEY LIFECYCLE



Key destruction is the removal of an encryption key from its operational location.

Key deletion goes further and removes any info that could be used to reconstruct that key.

EXAMPLE: (MS Intune, AirWatch)

MDM systems remove certificates from a device during device wipe or retirement.

CRYPTOGRAPHY & KEY MANAGEMENT

Other key management terms and concepts to know for the exam:

Level of Protection

Encryption keys must be secured at the same level of control or higher as the data they protect.

Sensitivity of the data dictates this level of protection, as defined in the organization's data security policies.

Key Recovery

Circumstances where you need to recover a key for a particular user, without that user's cooperation, such as in termination or key loss.

Key Escrow

Copies of keys held by a trusted third party in a secure environment, which can aid in many of the other areas of key management .

KEY MANAGEMENT IN THE CLOUD (CSPs - Azure, AWS, GCP)

Key Management System (KMS)

E.G. Azure Key Vault, AWS KMS, GCP Cloud KMS Vault

CSPs offer a cloud service for centralized secure storage and access for application secrets called a vault.

A secret is anything that you want to control access to, such as **API keys**, **passwords**, **certificates**, **tokens**, or **cryptographic keys.**

Service will typically offer programmatic access via API to support DevOps and continuous integration/continuous deployment (CI/CD)

Access control at vault instance-level and to secrets stored within.

Secrets and keys can generally be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

IDENTITY AND ACCESS CONTROL

In the cloud, services should include strong authentication mechanisms for validating users' identities and credentials

Provisioning and Deprovisioning

- Standardize, streamline, and develop an efficient account creation process
- Timely deprovisioning eliminates access sprawl

Centralized directory Services

- Active Directory and LDAP
- Kerberos and NTLM authentication

Privileged user management

- Managing privileged access accounts
- Enforce Least Privilege and Need to know
- Separation of duties can provide effective risk mitigation

Authentication and access management

- Focused on the manner in which users can access required resources

MULTI-ATTACK PREVENTION

Multi-factor Authentication

Something you **know** (pin or password)

Something you **have** (trusted device)

Something you **are** (biometric)

PREVENTS:

- Phishing
- Spear phishing
- Keyloggers
- Credential stuffing
- Brute force and reverse brute force attacks
- Man-in-the-middle (MITM) attacks

LIMITING ACCESS & DAMAGE

Need-to-know and the **principle of least privilege** are two standard IT security principles implemented in secure networks.

They limit access to data and systems so that users and other subjects have access only to what they require.

They help prevent security incidents

They help limit the scope of incidents when they occur.

When these principles are not followed, security incidents **result in far greater damage** to an organization.

PREVENTING FRAUD AND COLLUSION

Collusion is an agreement among multiple persons to perform some unauthorized or illegal actions.

Separation of duties

a basic security principle that ensures that no single person can control all the elements of a critical function or system.

Job rotation

employees are rotated into different jobs, or tasks are assigned to different employees.

Implementing these policies **helps prevent fraud** by limiting actions individuals can do without colluding with others.

ACCOUNT TYPES

Service Account aka "Service Principal"

when software is installed on a computer or server, it may require privileged access to run.

a lower-level administrative account, and the service account fits the bill.

a service account is a type of administrator account used to run an application. example: account to run an anti-virus application.

Shared Account

When a group of people performs the same duties, such as members of customer service, they can use a shared account.

when user-level monitoring, auditing, or non-repudiation are required, you must eliminate the use of shared accounts.

Most cloud IDPs have options to eliminate the need for shared accounts

PRIVILEGED ACCESS MANAGEMENT

a solution that helps protect the privileged accounts within a tenant, preventing attacks

also provides visibility into who is using privileged accounts and what tasks they are being used for

PRIVILEGED ACCESS MANAGEMENT

a solution that helps protect the privileged accounts within a tenant, preventing attacks

Native to some cloud identity providers today, and may include a just-in-time elevation feature

Less secure data destruction

Erasing. performing a delete operation against a file, files, or media.

Clearing (overwriting). preparing media for reuse and ensuring data cannot be recovered using traditional recovery tools.

May use random data or zeros, one or multiple passes

Purging. a more intense form of clearing that prepares media for reuse in less secure environments.

Media is reusable with any of these methods

Data may be recoverable with forensic tools

More secure data destruction

Crypto-shredding "cryptographic erasure"

1. Data is encrypted with a strong encryption engine.
2. The keys used to encrypt the data are then encrypted using a different encryption engine.
3. Then, keys from the second round of encryption are destroyed.

PRO: Data cannot be recovered from any remnants.

CON: High CPU and performance overhead

If the exam poses questions on "secure data Destruction", this is almost certainly the answer!

Destroying Media Data

Destroying data on media such as a hard drive or DVD/CD ROM

Degaussing. creates a strong magnetic field that erases data on some media and destroy electronics.

Shredding. You can shred a metal hard drive into powder.

Pulverizing. Use a hammer and smash drive into pieces, or drill through all the platters.

Media is not reusable with any of these methods

Data is also not recoverable by any means

NETWORK SECURITY

Network security groups provide an additional layer of security for cloud resources

Act as a virtual firewall for virtual networks and resource instances. (e.g. VMs, databases, subnets)

Carries a list of security rules (IP and port ranges) that allow or deny network traffic to resource instances.

Provides a virtual firewall for a collection of cloud resources with the same security posture.

Exists in multiple CSPs. Details may vary slightly with each.

CLOUD SECURITY CONTROLS - NETWORK

Segmentation

Restricting services that are permitted to access or be accessible from other zones using rules to control inbound/outbound traffic.

Rules are enforced by the IP address ranges of each subnet.

Within a virtual network, segmentation can be used to achieve isolation. Port filtering through a network security group

API inspection and integration:

Representational State Transfer (REST) is the modern approach to writing web service APIs.

Enables multi-language support, can handle multiple types of calls, return different data formats.

APIs published by an organizations should include encryption, authentication, rate limiting, throttling, and quotas.

Traffic Inspection

Packet capture in the cloud generally requires tools designed for this purpose in the environment.

Traffic is often sent direct to resources and promiscuous mode on a VM NIC not possible or effective.

EXAMPLES: Network Watcher (Azure), VPC traffic mirroring (AWS)

CSPs offering tools to facilitate packet capture within customer tenant

GEOFENCING

Uses the Global Positioning System (GPS) or RFID to define geographical boundaries.

Once the device is taken past the defined boundaries, the security team will be alerted.

EXAMPLES:

Restrict access to systems and services based on where the access attempt is being generated from.

Prevent devices from being removed from the company's premises.

Identifies unusual traffic patterns and prevents misuse.

Zero Trust Security

no entity is trusted by default!

Addresses the limitations of the legacy network perimeter-based security model.

Treats user identity as the control plane

Assumes compromise / breach in verifying every request.

ZERO TRUST PRINCIPLES

Verify explicitly. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least privilege access. Limit user access with just-in-time and just-enough-access (JIT and JEA), risk-based adaptive policies, and data protection

Assume breach. Segment access to minimize scope of impact. Verify end-to-end encryption, use analytics to get visibility, drive threat detection, and improve defenses.

Zero Trust Security

no entity is trusted by default!

Addresses the limitations of the legacy network perimeter-based security model.

Treats user identity as the control plane

Assumes compromise / breach in verifying every request.

ZERO TRUST NETWORK ARCHITECTURE

-Network Security Group (NSG)
-Network **Firewalls**
-Inbound and outbound **traffic filtering**
-Inbound and outbound **traffic inspection**
-Centralized **security policy** management and enforcement

Containerization

Examples include Docker and Kubernetes

A lightweight, granular, and portable way to package applications for multiple platforms.

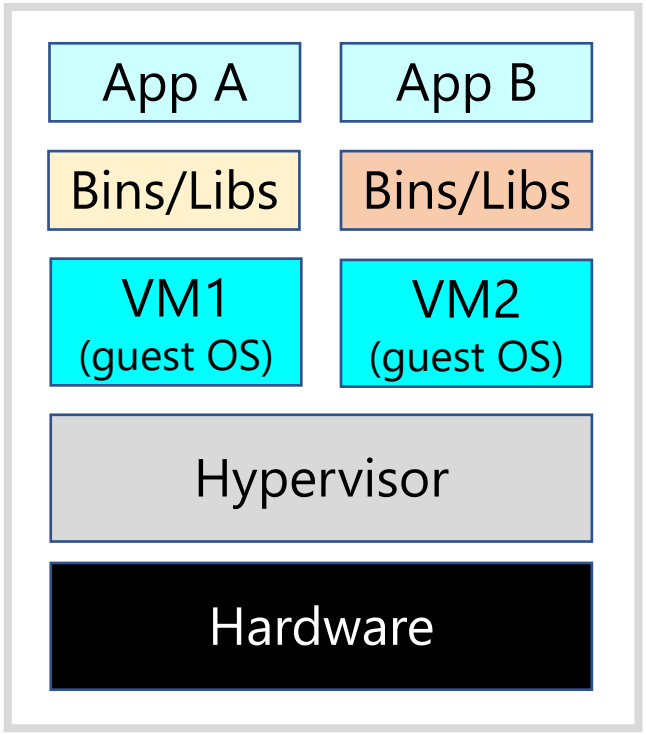
Reduces overhead of server virtualization by enabling containerized apps to run on a shared OS kernel.

containers do not have their own OS !

Can be used in some cases to isolate existing applications developed to run in a VM with a dedicated operating system.

TYPE 1 HYPERVISOR

"Bare metal"

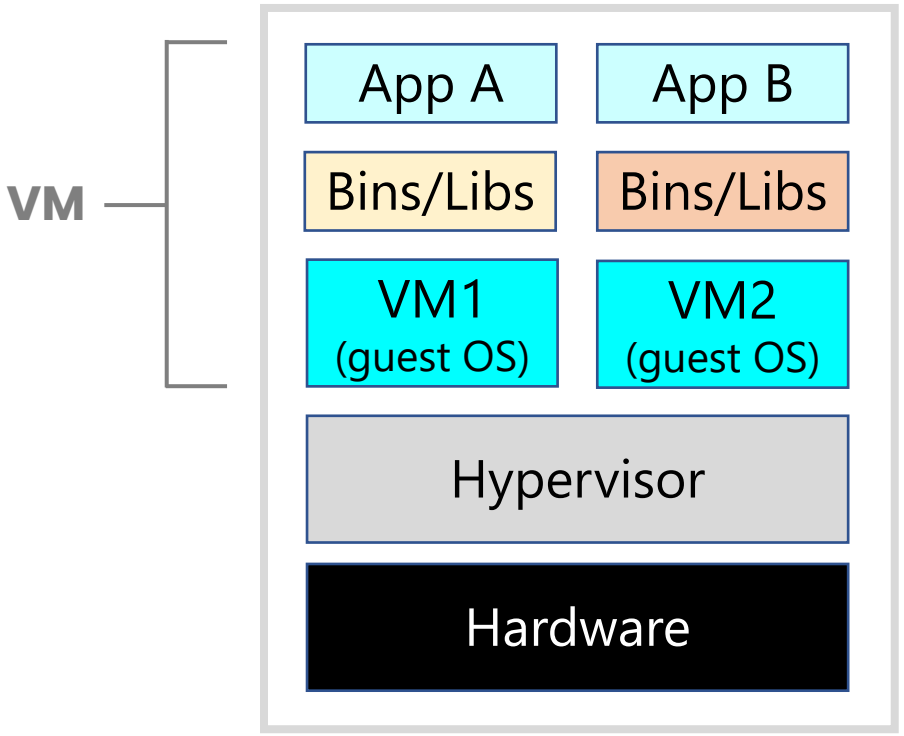


VMware ESXi, KVM
Microsoft Hyper-V

VIRTUALIZATION SECURITY: **CONTAINERS**

TYPE 1 HYPERVISOR

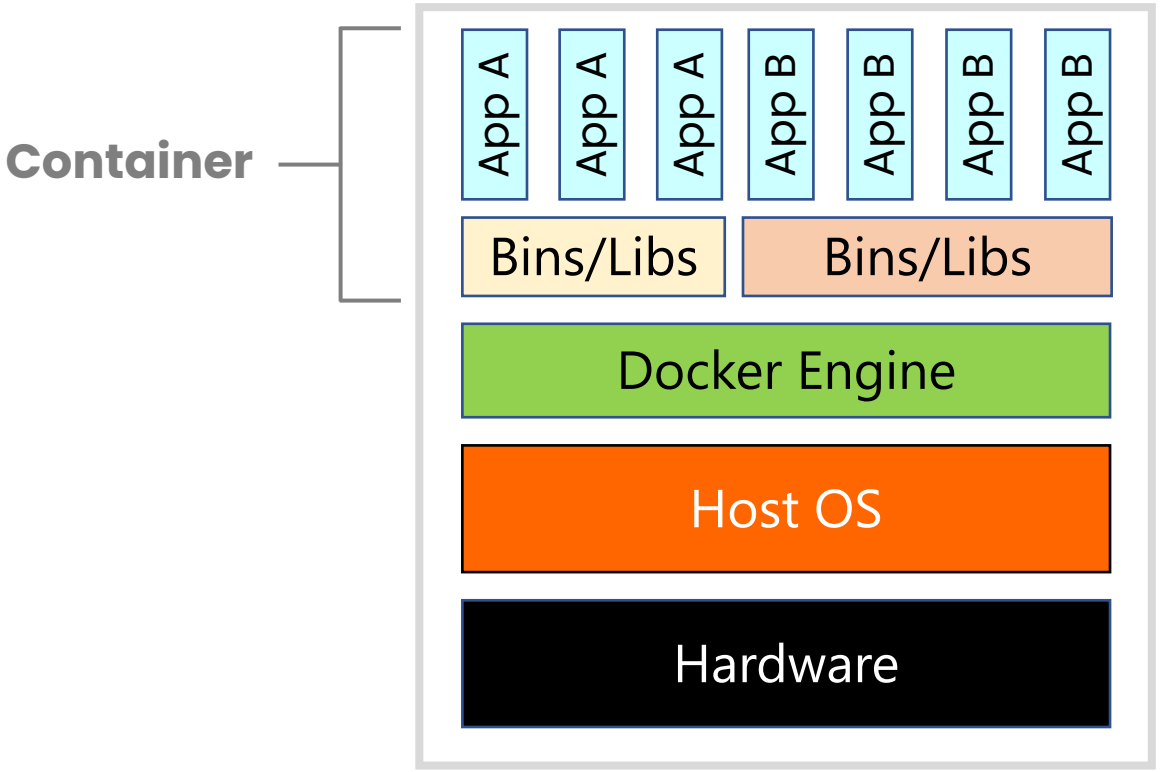
"Bare metal"



Each VM has its own OS kernel and memory, resulting in more overhead

CONTAINER HOST

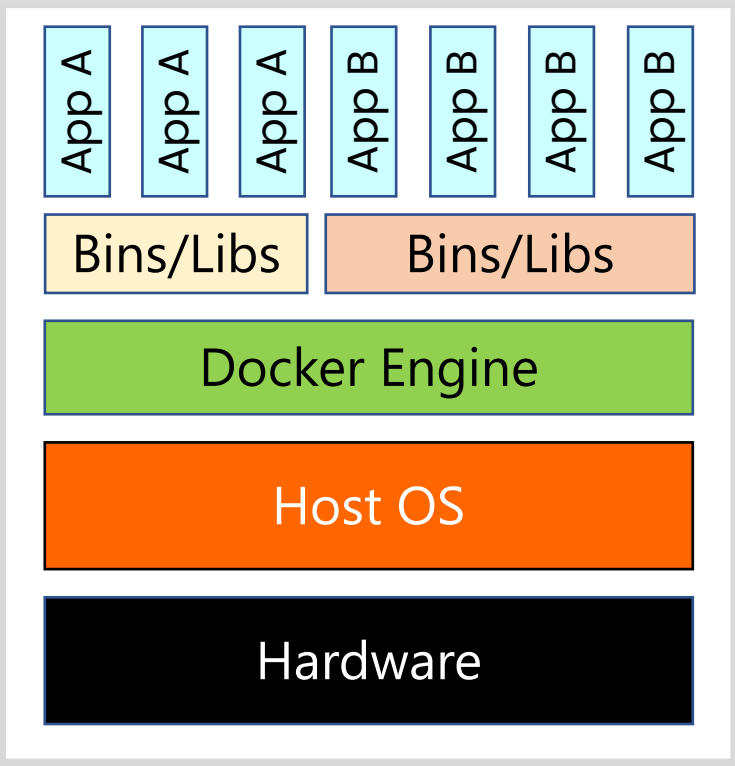
Usually, a cloud VM



Containers are isolated, but share a single OS kernel, as well as bins/libs where possible

CONTAINER HOST

Usually, a cloud VM

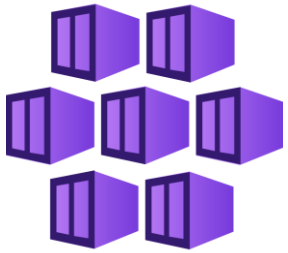


Core components in a container platform (Docker, Kubernetes):

- -Orchestration/scheduling controller
- -Network, storage
- -Container host
- -Container images
- -Container registry

The isolation is logical, isolating processes, compute, storage, network, secrets, and management plane

CONTAINER SECURITY



Managed Kubernetes

Container hosts are cloud-based virtual machines (VM). This is where the containers run

Most CSPs offer **hosted Kubernetes service**, handles critical tasks like health monitoring and maintenance for you. Platform-as-a-Service

You pay only for the agent nodes within your clusters, not for the management cluster.

Major CSPs also offer a monitoring solution that will identify at least some potential security concerns

EXAMPLES: AKS (MSFT), EKS (AWS), GKE (GCP)

Shares many of the concerns of server virtualization, but must enforce **isolation** of network, data, storage access at container-level.

VIRTUALIZATION SECURITY

Serverless Technology

Described in section 1.2 earlier in this video

Use API gateways as security buffers (to avoid DDoS attacks)

Configure secure authentication (Oauth, SAML, OpenID Connect, MFA)

Separate dev and prod environments, implement least privilege

Ephemeral Computing

the practice of creating a virtual computing environment as a need arises.

environment is destroyed once needs are met, and resources are no longer needed

Used in autoscaling (elasticity)

COMMON THREATS

Data Breach *The result of a cyberattack*

When sensitive data is stolen, including personally identifiable information (PII) and protected health information (PHI).

Often due to poor application or database security design or configuration, whereby data is exposed without proper authorization.

Preventable by following secure development practices and adhering to recommendations in the **secure data lifecycle**

Data Loss *Sometimes called "data leaks"*

When sensitive data is unknowingly exposed to the public

Often through a system or service misconfiguration or oversharing.

APIs (SOAP or REST)

is a set of exposed interfaces that allow programmatic interaction between services.

An avenue for security breach if not properly implemented

REST uses the HTTPS protocol for web communications to offer API end points Makes it a target for DDoS attacks

Security mechanisms include API gateway, authentication, IP filtering, throttling, quotas, data validation

Also ensure that storage, distribution, and transmission of **access keys** is performed in a secure fashion.

COMMON THREATS

Malicious Insiders

Disgruntled employees can wreak havoc on a system.

Internal acts of disruption include **theft** and **sabotage**.

Account or Service Traffic Hijacking

When attacks are designed to steal or wedge themselves into the middle of a conversation in order to gain control.

COMMON THREATS

Abuse of cloud services

Consumers sometimes misuse their cloud services for illegal or immoral activities.

Insufficient due diligence

Process/effort to collect and analyze information before making a decision or conducting a transaction.

Failure to perform due diligence can result in a due care violation.

Knowing the difference between due diligence and due care is important knowledge for your career

DUE DILIGENCE vs DUE CARE

Due Diligence | Process/effort to collect and analyze information before making a decision or conducting a transaction.

Due Care | Doing what a reasonable person would do in a given situation. It is sometimes called the "prudent person rule".

Together, these will reduce senior management's **culpability & (downstream) liability** when a loss occurs.

Decision

Research
Planning
Evaluation

Implementation
Operation (upkeep)
Reasonable measures

INCREASES understanding and **REDUCES** risk

"PRUDENT PERSON RULE"

Largely before the decision

DUE DILIGENCE

Doing after the decision

DUE CARE

BEFORE

Decision

Think **BEFORE** you act!

Do Detect

DUE DILIGENCE

AFTER

Actions speak louder than words

Do Correct

DUE CARE

BEFORE

Decision

AFTER

EXAMPLES

Knowledge and research of:

- ✓ Laws and Regulations
- ✓ Industry standards
- ✓ Best practices

EXAMPLES

Delivery or execution including:

- ✓ Reporting security incidents
- ✓ Security awareness training
- ✓ Disabling access in a timely way

DUE DILIGENCE

DUE CARE

COMMON THREATS

Shared Technology Vulnerabilities

The underlying infrastructure of the public cloud was not originally designed for the types of multitenancy in the public cloud

Modern virtualization software bridges most of the gaps

What threats remain in shared public cloud infrastructure?

Cloud infrastructure can still be vulnerable to insider threats

Unintentional misconfigurations are also a concern

To a lesser degree, disruptive attacks of scale (DoS, DDoS) and "noisy neighbors"

For regulatory compliance and high-criticality scenarios, CSPs have some higher isolation and flexible scale-out options.

Configuration & Change Management

Can prevent security related incidents and outages

Configuration Management

ensures that systems are configured similarly, configurations are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Change Management

helps reduce outages or weakened security from unauthorized changes to the baseline configuration.

Versioning uses a labeling or numbering system to track changes in updated versions of baseline (image, application, system, etc).

requires changes to be requested, approved, tested, and documented.

aka "Update Management"

What is Patch Management ?

The process of identifying, acquiring, installing, and verifying patches for products and systems.

It is a function included in change management.

Patches correct security and functionality problems in software and firmware.

Both applicability and install are automated with management tools

An **applicability assessment** is performed to determine whether a particular patch or update applies to a system.

1. CLOUD CONCEPTS, ARCHITECTURE, AND DESIGN

1.4 Understand Design Principles of Secure Cloud Computing

Cloud Secure Data Lifecycle

Cloud-based Business Continuity (BC) and Disaster Recovery (DR) Plan

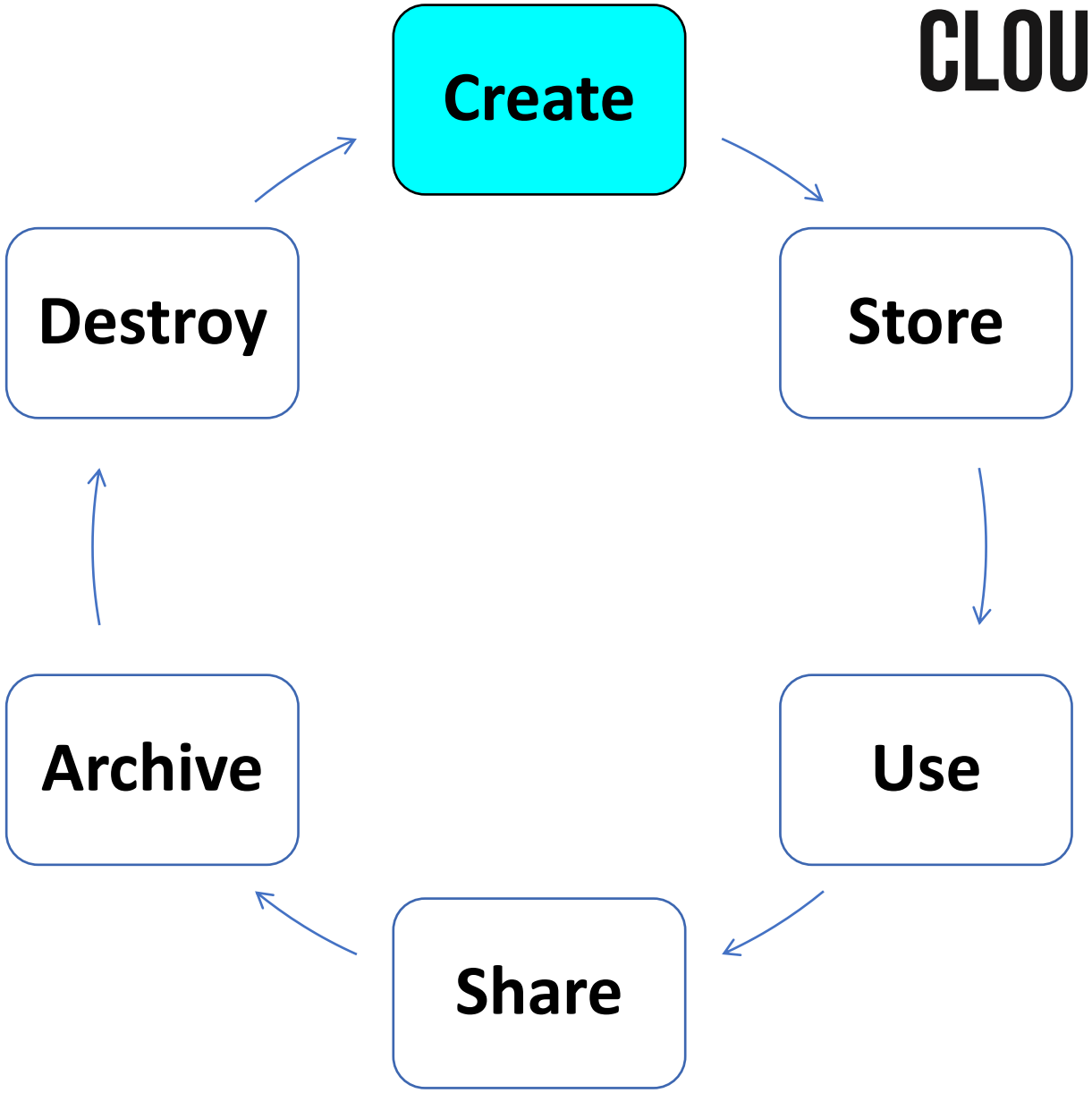
Business Impact Analysis (BIA)
(e.g., cost-benefit analysis, return on investment (ROI))

Functional Security Requirements
(e.g., portability, interoperability, vendor lock-in)

Security Considerations & Responsibilities for Different Cloud Categories
(e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

DevOps Security

CLOUD SECURE DATA LIFECYCLE



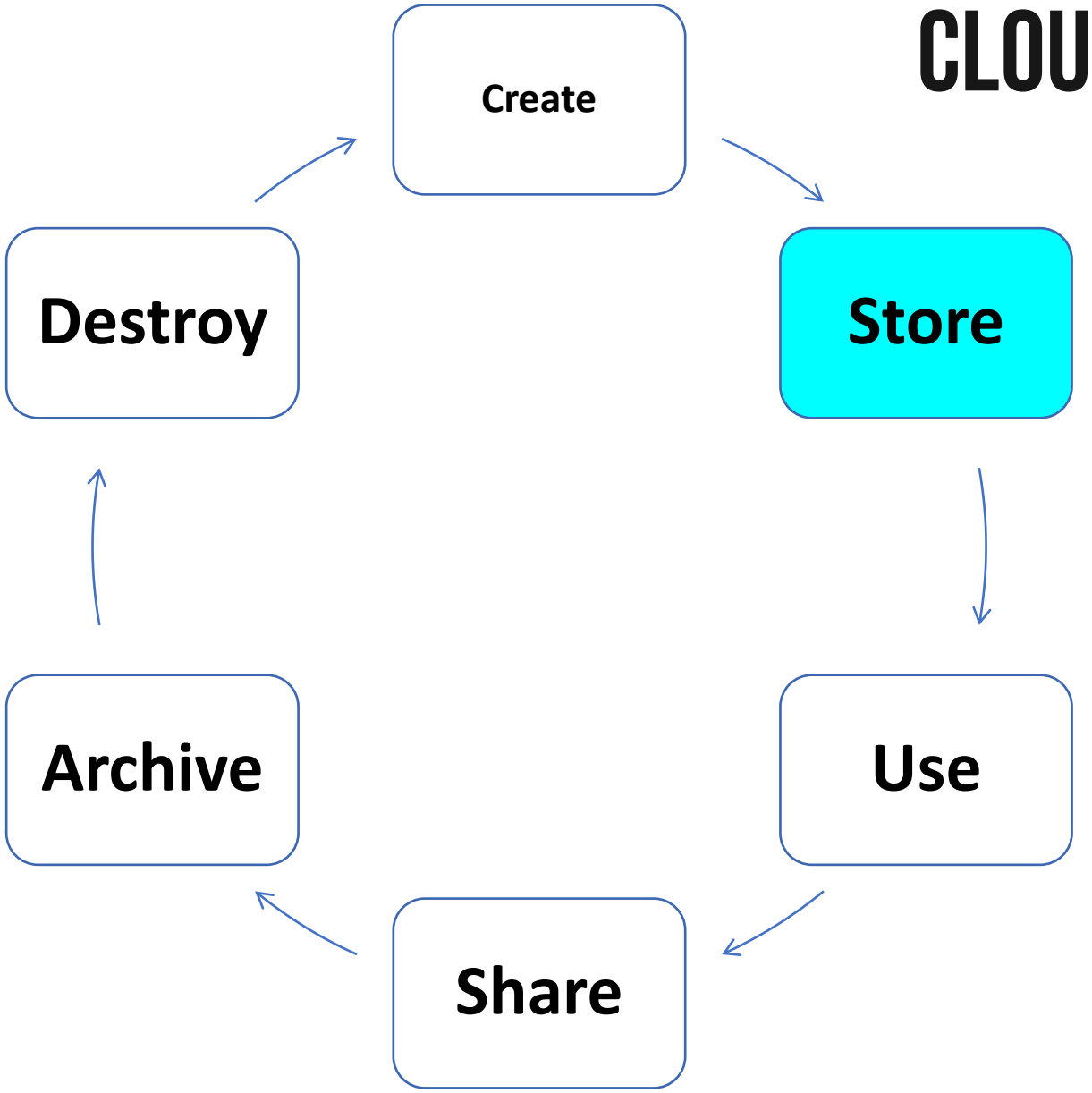
Can be created by **users**

a user creates a file

Can be created by **systems**

a system logs access

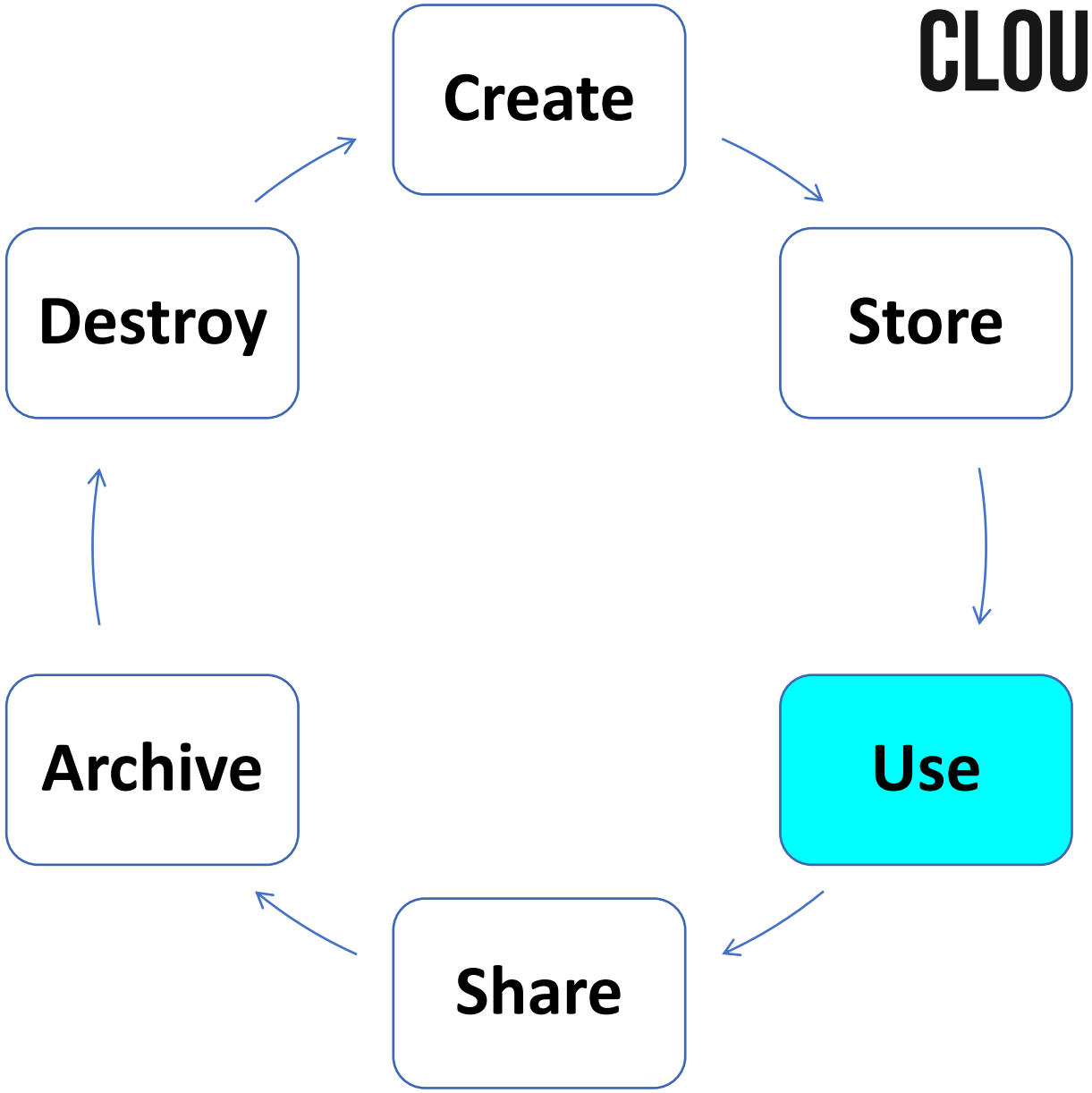
CLOUD SECURE DATA LIFECYCLE



To ensure it's handled properly, it's important to ensure data is **classified** as soon as possible.

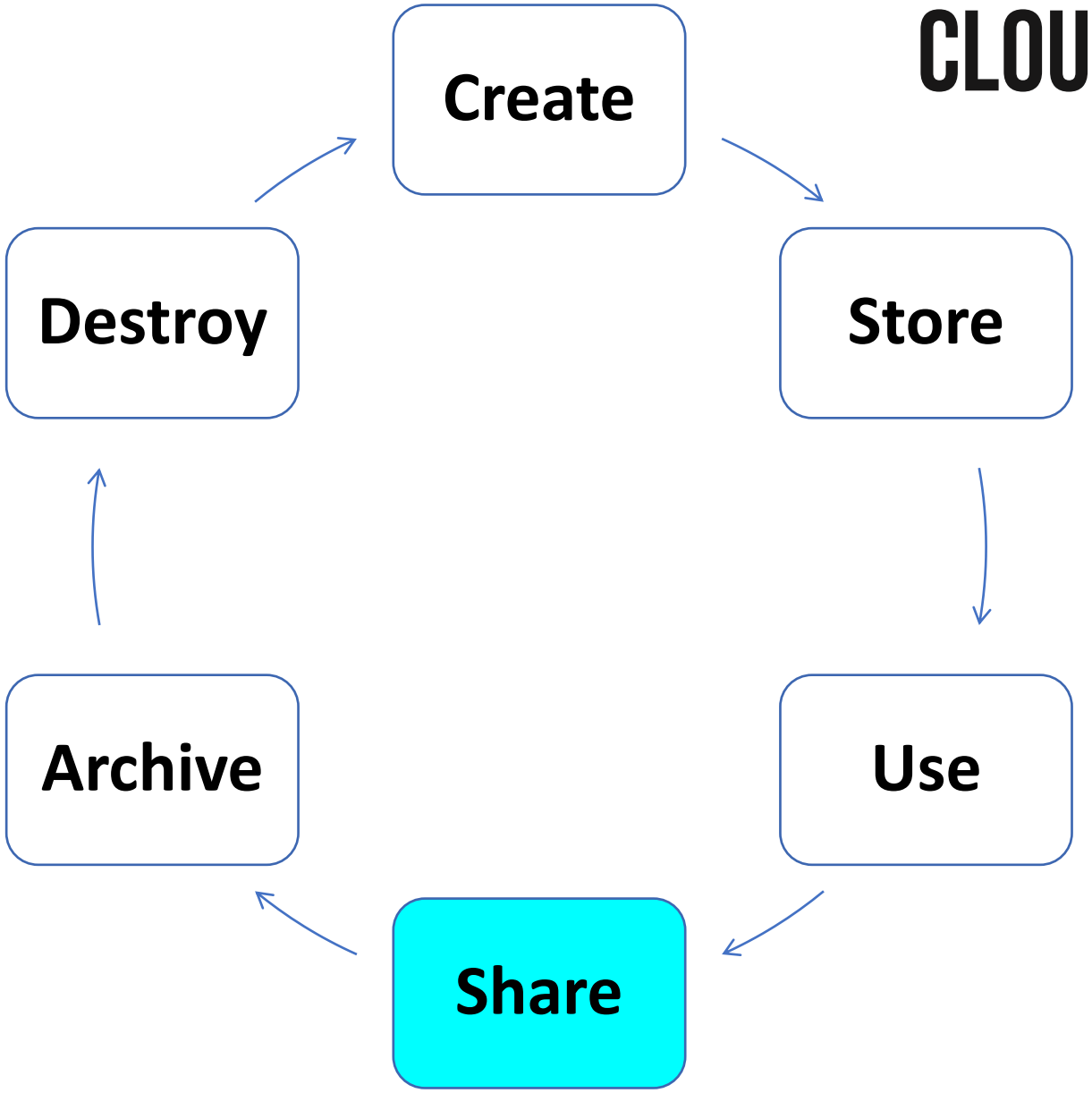
Ideally, data is encrypted at rest

CLOUD SECURE DATA LIFECYCLE



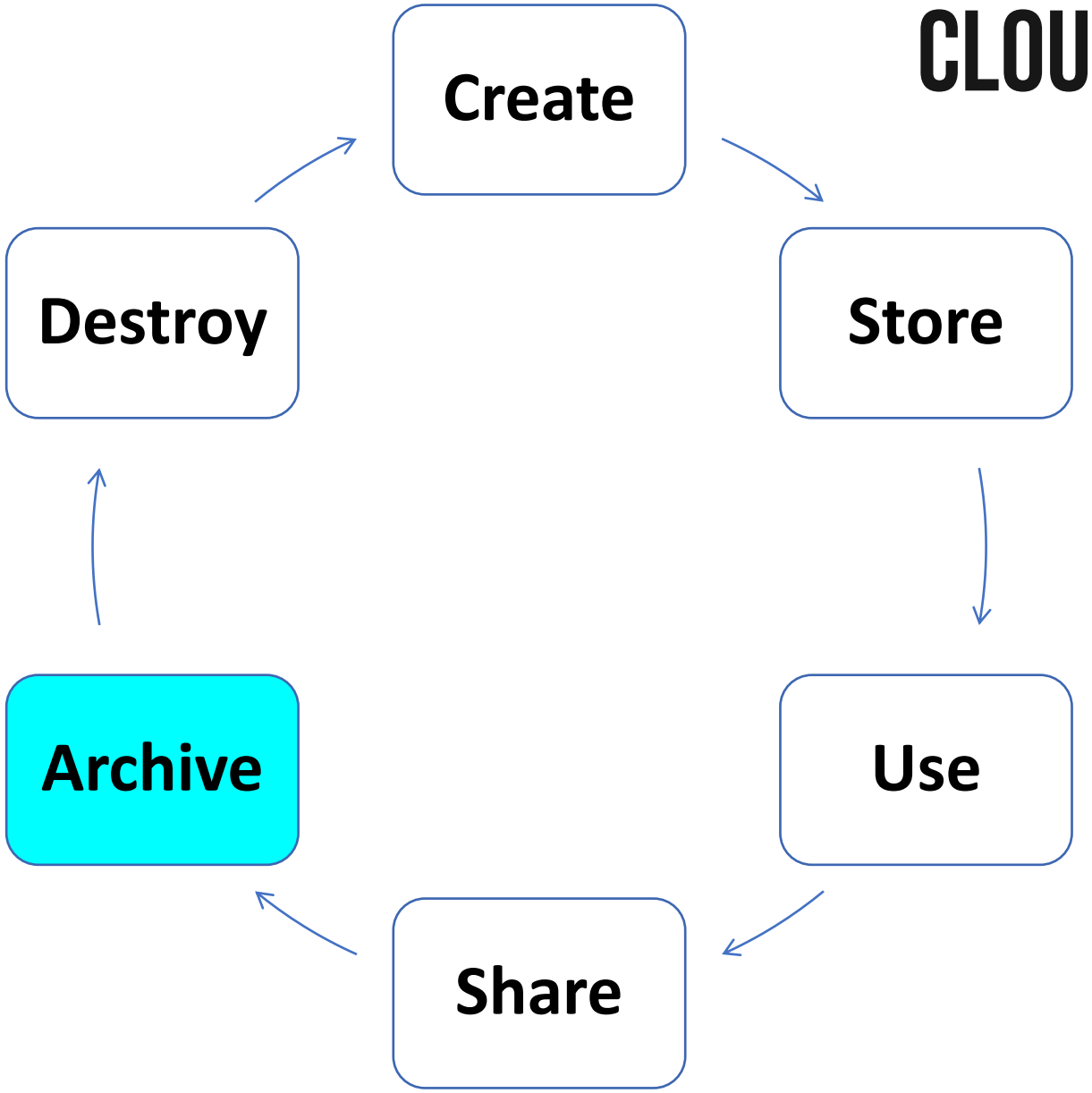
Data should be **protected** by adequate security controls based on its classification.

CLOUD SECURE DATA LIFECYCLE



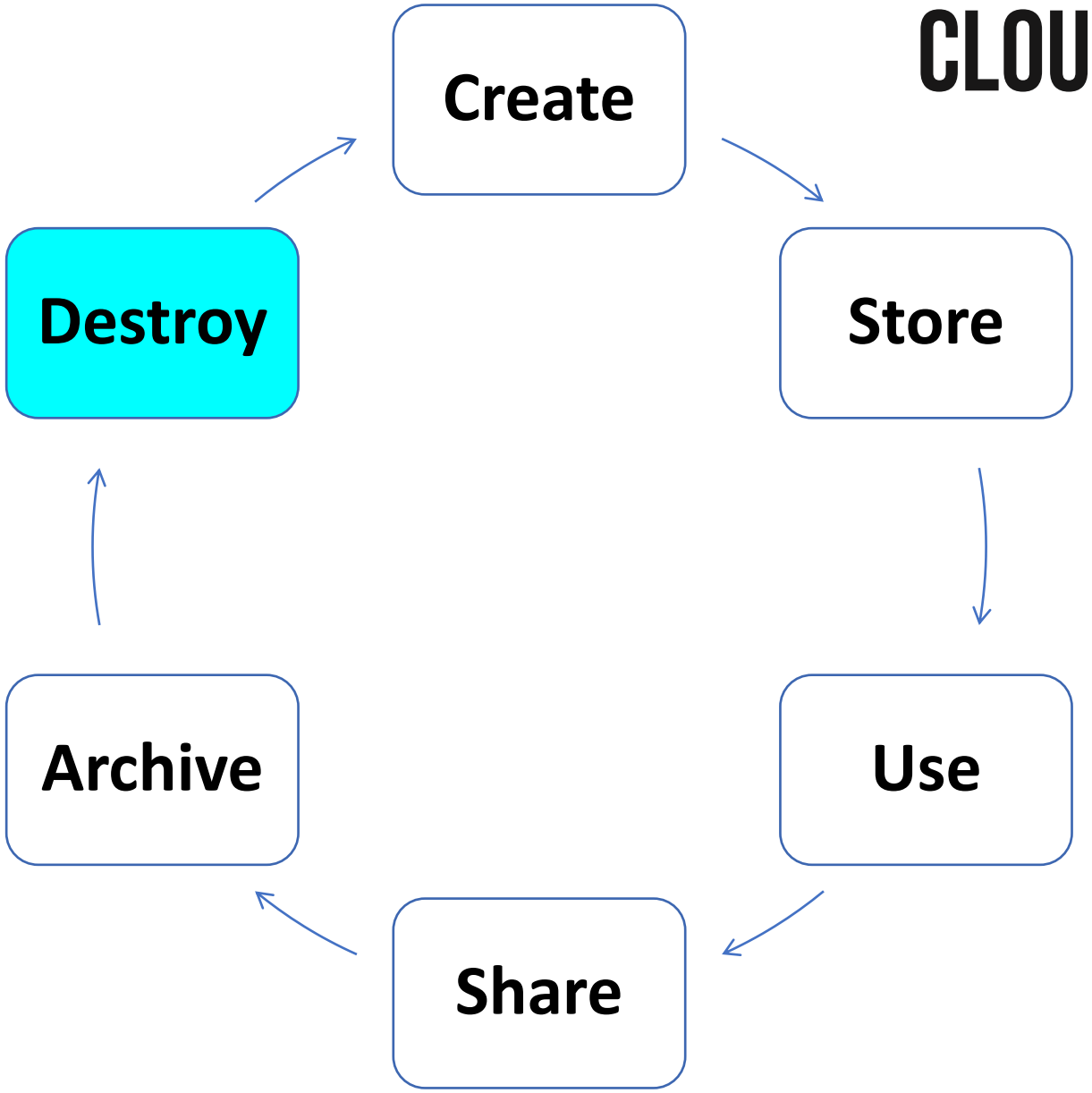
refers to anytime data is in use or in transit over a network

CLOUD SECURE DATA LIFECYCLE



archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

CLOUD SECURE DATA LIFECYCLE



When data is no longer needed, it should be destroyed in such a way that it is not readable nor recoverable.

Crypto-shredding happens in this phase!

DATA STATES

In transit

Data on the wire, in flight

Commonly protected with TLS or tunneled through VPN

At rest

In storage (on disk, in database, etc)

Protected through encryption

In use

In memory (RAM, CPU, cache, etc.)

Should be flushed from memory when transaction is complete or system is powered down

PROTECTING DATA AT REST

How can we encrypt different types of data **at rest**?

Storage Service Encryption

CSPs usually encrypt by default

CSP storage providers usually protect data at rest by automatically encrypting before persisting it to managed disks, object, file, or queue storage.

Full Disk Encryption

helps you encrypt Windows and Linux IaaS VMs disks using BitLocker (Windows) and dm-crypt feature of Linux to encrypt OS and data disks.

Transparent data encryption (TDE)

Helps protect SQL Database and data warehouses against threat of malicious activity with real-time encryption and decryption of database, backups, and transaction log files at rest without requiring app changes.

Some database platforms also provide row-level encryption, column-level encryption, or data masking

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner

Holds the legal rights and complete control over a single piece of data.

Usually a member of **senior management**. Can delegate some day-to-day duties. CANNOT delegate total responsibility!

Data Custodian

Responsible for safe custody, transport, and storage of data, and implementation of business rules, technical controls. (CIA, audit trails, etc)

Usually someone in the **IT department**. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

GDPR Data Roles and Concepts

Two roles that appear in GDPR regulations

Data Processor. A natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller.

Data Controller. The person or entity that controls processing of the data.

In the OSG - may appear on the exam!

OTHER ROLES

Data Subject

Refers to any individual person who can be identified, directly or indirectly, via an identifier

Identifiers may include name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

Data Steward

Ensure the data's context and meaning are understood, and business rules governing the data's usage.

Use that knowledge to ensure the data they are responsible for is used as intended.

BCP DEFINITIONS

Some BCP-related definitions worth knowing

BCP (Business Continuity Plan)
the overall organizational plan for "how-to" continue business.

DRP (Disaster Recovery Plan)

the plan for recovering from a disaster impacting IT and returning the IT infrastructure to operation.

BCP vs DRP

Business Continuity Planning (BCP) vs Disaster Recovery Planning (DRP) – What is the difference?

BCP focuses on the whole business

DRP focuses more on the technical aspects of recovery

BCP will cover communications and process more broadly

BCP is an umbrella policy and DRP is part of it

DISASTER RECOVERY IN THE CLOUD

Disaster Recovery is built into cloud architecture

Region Pairs addresses site-level failure

Region pairs are 300+ miles apart, selected by CSP

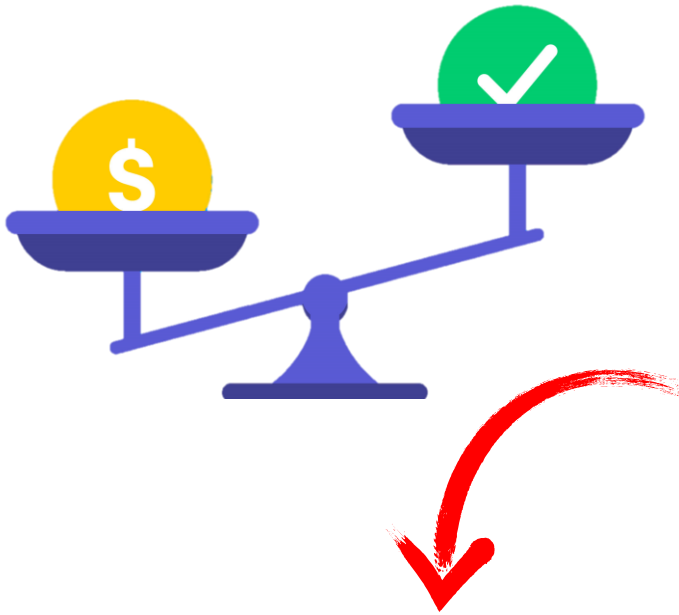
Availability Zones address datacenter failures within a cloud region

A CSP region (e.g. East US) includes multiple datacenters

Availability sets address rack-level failures within a regional datacenter

Consists of two or more 'fault domains' for power, network, etc.

BUSINESS IMPACT ANALYSIS



A **business impact analysis (BIA)** contains two important items:

✓ a cost-benefit analysis (CBA) AND

✓ a calculation of the return on investment (ROI)

A **cost-benefit analysis** lists the benefits of the decision alongside their corresponding costs.

CBA can be strictly quantitative: adding the financial benefits and subtracting the associated costs to determine whether a decision will be profitable.

A thorough cost-benefit analysis will consider intangible benefits (those you cannot calculate directly).

FUNCTIONAL SECURITY REQUIREMENTS

Functional vs Non-Functional security requirements

What is the difference?

Functional security requirements

Define a system or its component and specifies what it must do.

Captured in use cases, defined at a component level.

EXAMPLE: application forms must protect against injection attacks.

Non-functional security requirements

Specify the system's quality, characteristics, or attributes.

Apply to the whole system (system level)

EXAMPLE: security certifications are non-functional.

SECURITY CONSIDERATIONS FOR DIFFERENT CLOUD CATEGORIES

IaaS

VM attacks

Virtual network

Hypervisor attacks

VM-based rootkits

Virtual switch attacks

Colocation

DoS attack

PaaS

System and Resource Isolation

User-Level Permissions

Access Management

Protection Against Malware, Backdoors, and Trojans

SaaS

Data Segregation

Data Access and Policies

Web Application Security

See "shared responsibility model"

Attack surface, shared responsibility, and data sensitivity all influence attack and defense strategies

VIRTUALIZATION-FOCUSED ATTACKS

VM Escape

where an attacker gains access to a VM, then attacks either the host machine that holds all VMs, the hypervisor, or any of the other VMs.

Protection: ensure patches and hypervisor and VMs are always up to date, guest privileges are low. Server-level redundancy and HIPS/HIDS protection also effective.

VM Sprawl

When unmanaged VMs have been deployed on your network. Because IT doesn't know it is there, it may not be patched and protected, and thus more vulnerable to attack

Avoidance: enforcement of security policies for adding VMs to the network, as well as periodic scanning to identify new virtualization hosts.

These apply to both VMs and VM container hosts

APPLICATION ATTACKS

attacks attackers use to exploit **poorly written software**.

Rootkit (escalation of privilege)

freely available on the internet and exploit known vulnerabilities in various operating systems enabling attackers to elevate privilege.

keep security patches up-to-date
anti-malware software, EDR/XDR

Back Door

undocumented command sequences that allow individuals with knowledge of the back door to bypass normal access restrictions.
often used in development and debugging.

countermeasures:
firewalls, anti-malware, network monitoring, code review

NETWORK ATTACKS

These are a class of attacks

Denial of-Service | is a resource consumption attack intended to prevent legitimate activity on a victimized system.

Distributed **Denial of-Service** | a DoS attack utilizing multiple compromised computer systems as sources of attack traffic.

COUNTERMEASURES: firewalls, routers, intrusion detection (IDS), SIEM, disable broadcast packets entering/leaving, disable echo replies, patching

TYPES OF DDoS ATTACKS

Cloud service providers (MSFT, AWS) have DDoS protection built-in

Network

volume-based attacks targeting flaws in network protocols, often using botnets, using techniques such as UDP, ICMP flooding, or SYN flooding (TCP-based).

Application

exploit weaknesses in the application layer (Layer 7) by opening connections and initiating process and transaction requests that consume finite resources like disk space and available memory.

Operational Technology (OT)

Targets the weaknesses of software and hardware devices that control systems in factories, power plants, and other industries, such as IoT devices.

Often target weaknesses using the network and application techniques described above.

COUNTERMEASURES: IDS, IPS, rate-limiting, firewall ingress/egress filters

DEVOPS SECURITY

DevOps relies heavily on deployment automation for **Continuous integration/continuous delivery (CI/CD)**

Security controls should be implemented to mitigate risks

Technical

- ✓ Automated software scanning
- ✓ Automated vulnerability scanning
- ✓ Web application firewall
- ✓ Software dependency management
- ✓ Access and activity logging
- ✓ Application performance management

Administrative

- ✓ Developer application security training
- ✓ Documented policies and procedures
- ✓ Code review, approval gates

1.5 Evaluate Cloud Service Providers

Verification Against Criteria

(e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS))

System/subsystem Product Certifications

(e.g., Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)

ISO/IEC 27017:2015

Provides guidelines for information security controls applicable to the provision and use of cloud services

Provides cloud-based guidance on several ISO/IEC 27002 controls, along with seven cloud controls that address:

1) Who is responsible for what between the cloud service provider and the cloud customer
2) The removal/return of assets when a contract is terminated
3) Protection and separation of the customer's virtual environment
4) Virtual machine configuration
5) Administrative operations and procedures associated with the cloud environment
6) Customer monitoring of activity within the cloud
7) Virtual and cloud network environment alignment

PCI DSS

Payment **C**ard **I**ndustry
Data **S**ecurity **S**tandard

a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions

created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express

BASED ON 6 MAJOR OBJECTIVES

- a secure network must be maintained in which transactions can be conducted
- cardholder information must be protected wherever it is stored
- systems should be protected against the activities of malicious hackers
- cardholder data should be protected physically as well as electronically.
- networks must be constantly monitored and regularly tested
- a formal information security policy must be defined, maintained, and followed

SYSTEM PRODUCT CERTIFICATIONS

Common Criteria (ISO/IEC 15408)

Enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements.

Ensures customers that security products they purchase have been thoroughly tested by independent third-party testers

...and meets customer requirements.

The certification of the product only certifies product capabilities.

Designed to provide assurances for security claims by vendors

If misconfigured or mismanaged, software is no more secure than anything else the customer might use.

FIPS 140-2

Federal **I**nformation
Processing **S**tandard

Established to aid in the protection of digitally stored unclassified, yet sensitive, information

Developed by NIST, for use in computer systems by non-military American government agencies and government contractors

FIPS Security Levels

Remember these for the exam!

- **Level 1:** Lowest level of security.
- **Level 2:** Specifies the security requirements for cryptographic modules that protect sensitive information.
- **Level 3:** Requires physical protections to ensure a high degree of confidence that any attempts to tamper are evident and detectable

REFERENCE ARCHITECTURES

ARCHITECTURE

Documentation from CSPs and industry groups with guidance on cloud design and security

Cloud Service Providers

AWS Well-Architected Framework

Azure Well-Architected Framework

Google Cloud Architecture Framework

Industry Groups

Enterprise Architecture Reference Guide (Cloud Security Alliance)

Cloud Computing Reference Architecture (NIST)

Focus on architecture more than security

REFERENCE ARCHITECTURES

SECURITY

Documentation from CSPs and industry groups with guidance on cloud design and security

Cloud Service Providers

- Microsoft Cybersecurity Reference Architecture
- AWS Security Reference Architecture
- Google Cloud Security Foundations Guide

Industry Groups

- Enterprise Cloud Security Architecture (SANS)
- Security Technical Reference Architecture (CISA)
- Cloud Computing Security Reference Architecture (NIST)

Skimming SANS, CISA, and NIST docs may be helpful for exam

THANKS

FOR WATCHING!