CCSP

CCSP EXAM CRAM

EXAM PREPARATION SERIES

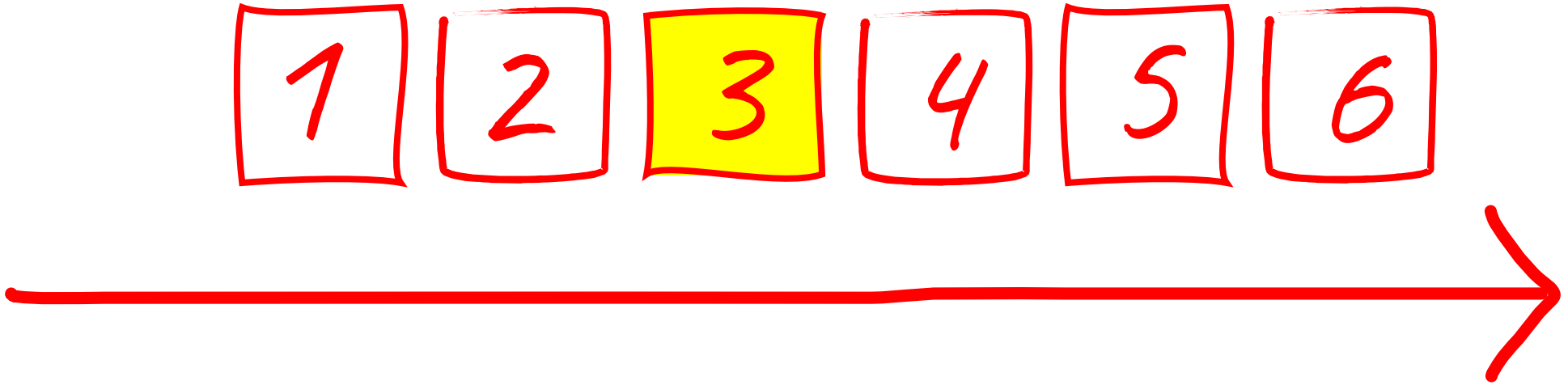
2023 EDITION

DOMAIN 3

Coverage of every topic in the official exam syllabus!

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 3 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 !

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 3

Cloud Platform and Infrastructure Security

I will cover every topic mentioned in the exam syllabus

INSIDE CLOUD AND SECURITY

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 3

Cloud Platform and Infrastructure Security

I will also provide examples of concepts when possible

INSIDE CLOUD AND SECURITY

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 3

Cloud Platform and Infrastructure Security

as well as a bit of show-and-tell
in a real cloud environment

INSIDE CLOUD
AND SECURITY

EXAM ESSENTIALS - 3

Risks associated with each type of cloud computing

More services = more risk, more control = more risks you must mitigate.

Explain key business continuity terms, like RTO, RPO, and RSL

Key concepts that help set the bar for your BCP/DRP requirements.

Responsibility sharing between customer and provider

Who is responsible (customer or CSP) in each area of cloud infrastructure.

Design and describe a secure datacenter

Build versus buy, physical and environment design considerations.

BC/DR in the cloud

Similar to on-premises, but more complexity in the agreements between cloud customer and cloud provider.

EXAM ESSENTIALS - 3

Exam essentials (and book chapters) in the Official Study Guide do not map one-to-one to exam domains

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.1 Comprehend Cloud Infrastructure and Platform Components

Physical environment

Network and communications

Compute

Virtualization

Storage

Management plane

In the shared responsibility model, customer and CSP share security responsibilities.

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.1 Comprehend Cloud Infrastructure and Platform Components

Physical environment

Network and communications

Compute

Virtualization

Storage

Management plane

We will review responsibilities and security controls with each area.

PHYSICAL ENVIRONMENT

There are infrastructure components that are common to all cloud service delivery models

Most components are all physically located with the CSP, but many are accessible via the network

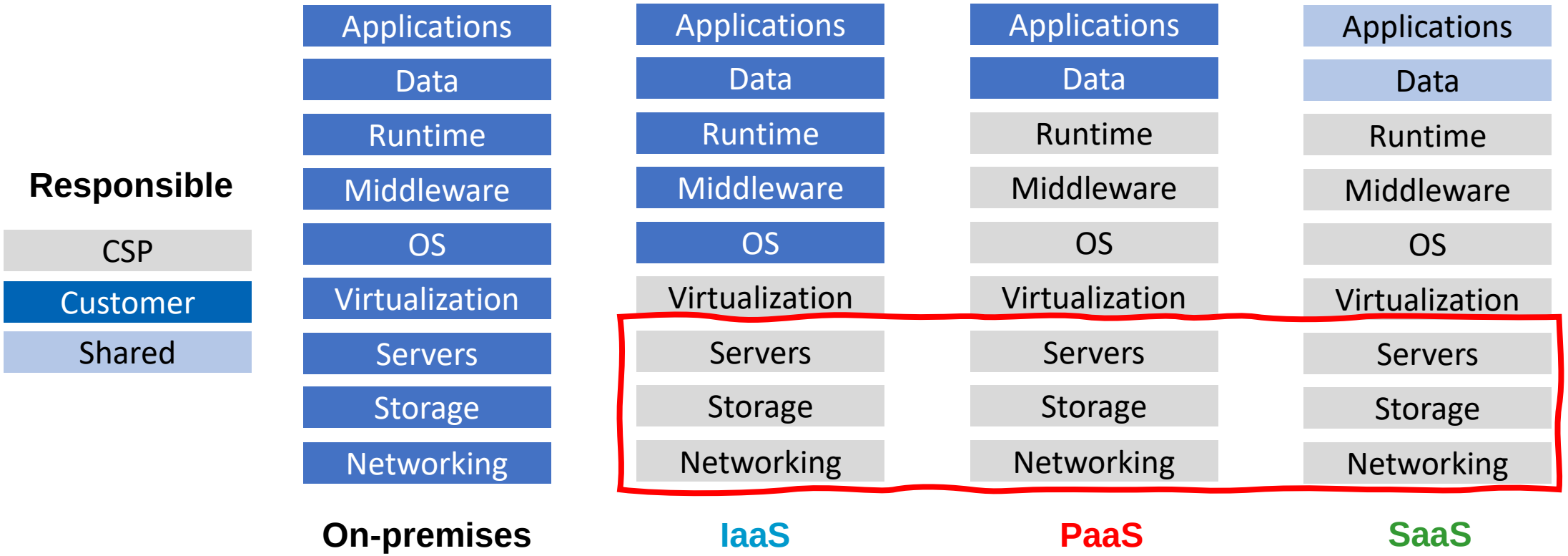
The CSP takes on customer datacenter facilities, infrastructure management responsibilities

In the shared responsibility model, some elements of operation are shared by the CSP and the customer.

For the exam, know who owns which roles from the "shared responsibility model"

SHARED RESPONSIBILITY MODEL

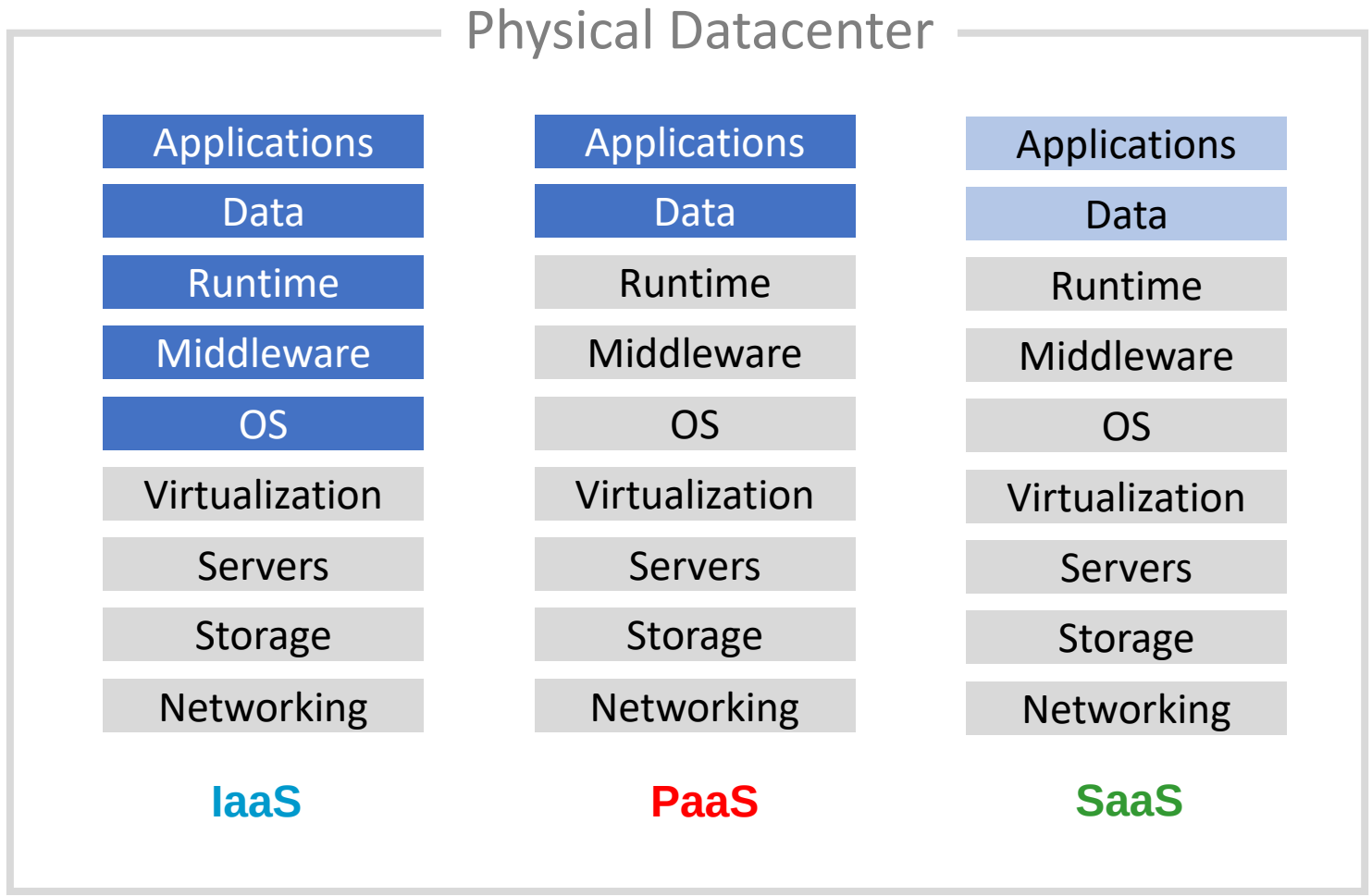
CSP owns all aspects of physical security in their datacenters



SHARED RESPONSIBILITY MODEL

Responsible

- CSP
- Customer
- Shared



Including datacenter **facilities**, **equipment**, and **environment**.

PHYSICAL ENVIRONMENT CONSIDERATIONS

CSPs utilize common controls to address these risks.

For physical security, standard measures such as locks, security personnel, lights, fences, visitor check-in procedures.

Logical access controls Identity and access management (IAM), single sign-on (SSO) provider, multifactor authentication (MFA) and logging.

Controls for data confidentiality and integrity like any cloud customer, but with much broader controls.

PHYSICAL ENVIRONMENT CONSIDERATIONS

CSPs utilize common controls to address these risks.

EXAMPLE

Ensuring that communication lines are not physically compromised by locating telecommunications equipment inside a controlled area of the CSP's building or campus.

Protects data integrity AND service/resource availability

NETWORK AND COMMUNICATION

IaaS
Infrastructure as a Service

Customer is responsible for configuring the VMs, virtual network, and guest OS security as if the systems were on-premises

CSP responsible for physical host, physical storage, and physical network

PaaS
Platform as a Service

CSP is responsible for the physical components, the internal network, and the tools provided.

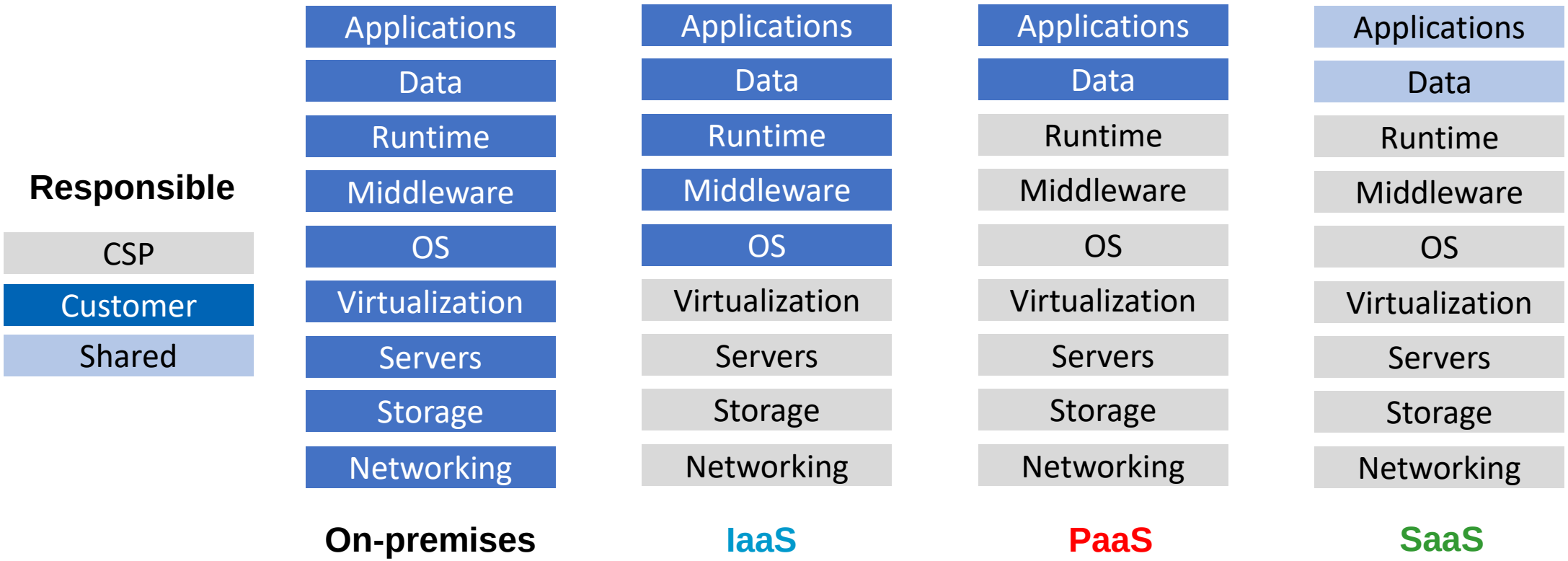
Cheaper for customer, but less control

SaaS
Software as a Service

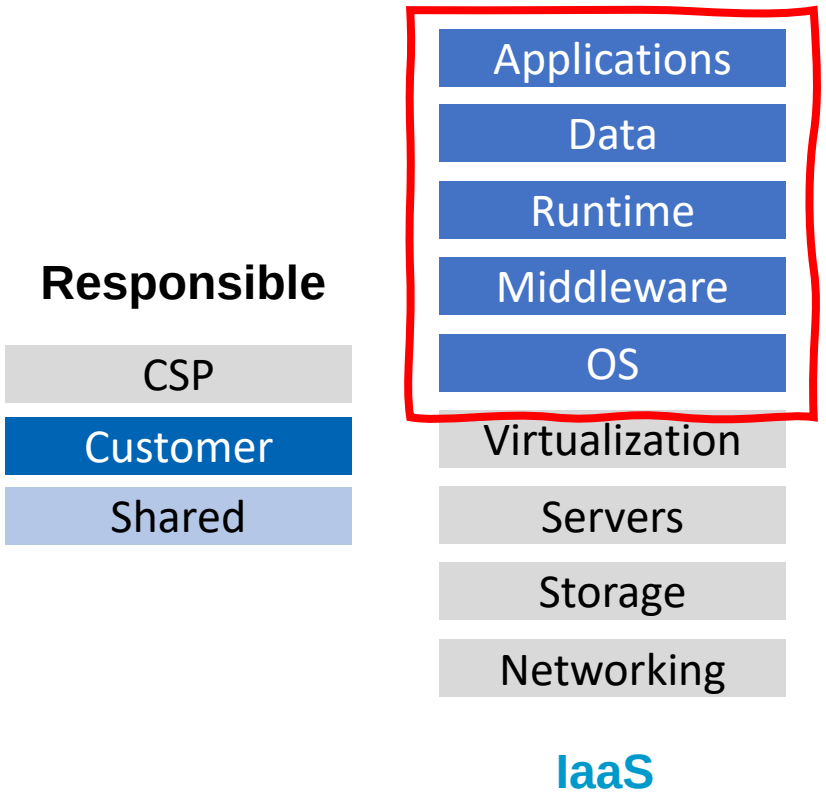
The customer remains responsible for configuring access to the cloud service for their users, as well as shared responsibility for data recovery

CSP owns physical infrastructure, as well as network and communication

SHARED RESPONSIBILITY MODEL



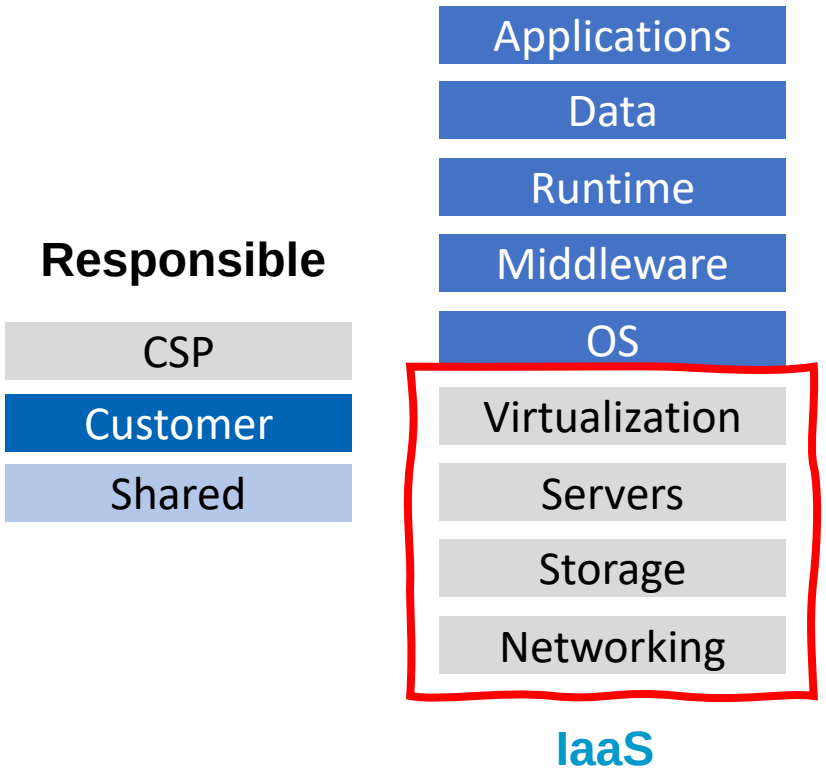
NETWORK AND COMMUNICATION - IAAS



Customer is responsible for configuring the VMs, virtual network, and guest OS security as if the systems were on-premises

CSP provides the tooling to secure the VM but customer must configure them!

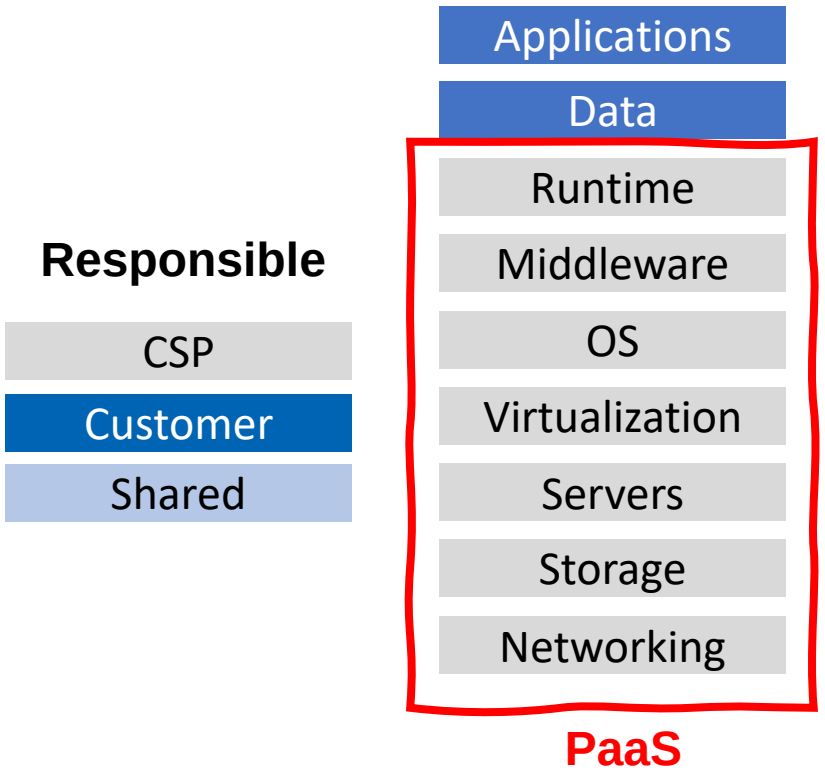
NETWORK AND COMMUNICATION - IAAS



CSP is responsible for configuring the security of the network, storage, and software for the physical host

CSP owns all physical security

NETWORK AND COMMUNICATION - PAAS



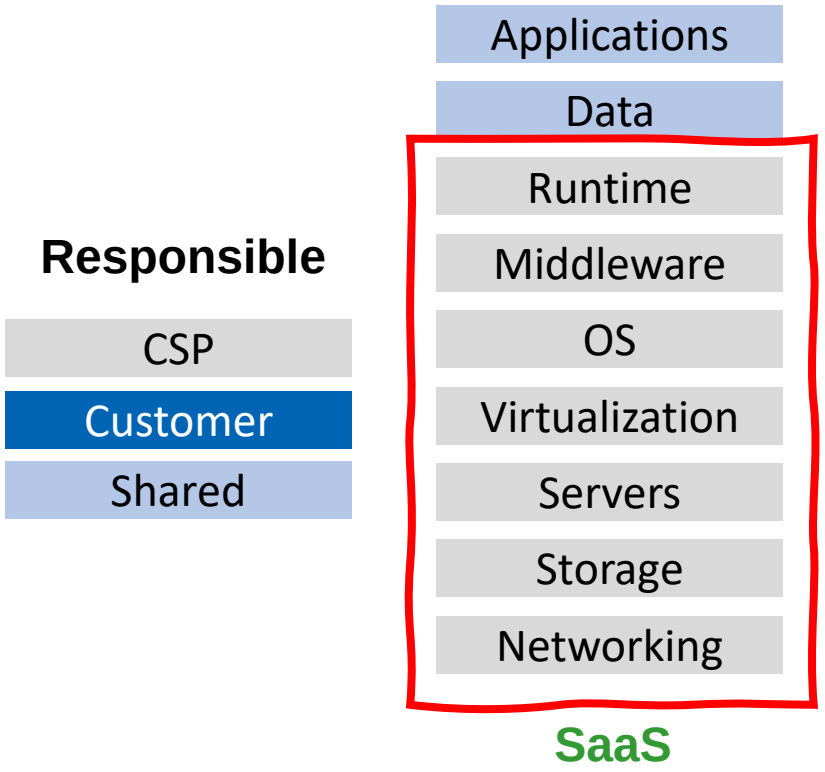
Customer is responsible for configuration of application and data access security

CSP is responsible for everything from the IaaS model (all the physical components),

CSP is responsible internal network, and the tools provided.

Any additional customer control is generally provided through service SKUs / tiers

NETWORK AND COMMUNICATION - SAAS



The customer remains responsible for configuring use access to the cloud service

Customer also has shared responsibility for data recovery ???

CSP may provide the tools for, but customer may need to perform recovery in some cases

EXAMPLE: Office 365 makes hundreds of previous versions of documents available for self-service recovery by users.

COMPUTE How does the CSP manage compute capacity?

The infrastructure components that deliver compute resources, such as the VMs, disk, processor, memory and network resources.

Reservation

a minimum resource that is guaranteed to a customer

Limits

maximum utilization of compute resource by a customer (e.g. VM)

limits are allowed to change dynamically based on current conditions and consumption

Shares

a weighting given to a particular VM used to calculate percentage-based access to pooled resources when there is contention.

In cases of shortage, host scoring determines who gets capacity

RESPONSIBILITY IN COMPUTE

the CSPs additional challenge is multitenancy.

In every delivery and service model:

The **CSP** remains responsible for the maintenance and security of the physical components of compute.

The **customer** remains largely responsible for their data and their users.

Between the physical components, there can be a large array of software and other components.

Who is responsible for each of these remaining parts varies by service and delivery model AND sometimes by the CSP.

The details should be spelled out in the contract!

VIRTUALIZATION - RESPONSIBILITIES AND RISKS

The security of the hypervisor is always the responsibility of the **CSP**.

The virtual network and virtual machine may be the responsibility of either the CSP or the customer.

It depends on the cloud service model

Risks associated with virtualization

- Flawed hypervisor can facilitate inter-VM attacks
- Network traffic between VMs is not necessarily visible
- Resource availability for VMs can be impacted
- VMs and their disk images are simply files, can be portable and movable

VIRTUALIZATION - RESPONSIBILITIES AND RISKS

Security recommendations for the hypervisor

- ✓ Install all updates to the hypervisor as they are released by the vendor.
- ✓ Restrict administrative access to the management interfaces of the hypervisor.
- ✓ Capabilities to monitor the security of activity occurring between guest operating systems (VMs).

All responsibility of the CSP

Security recommendations for the guest OS

- ✓ Install all updates to the guest OS promptly.
- ✓ Back up the virtual drives used by the guest OS on a regular basis

Customer responsibility, though CSP may provide tools

VIRTUALIZATION – NETWORK SECURITY

The CSP's **hypervisor security** includes:

-preventing physical access to the servers.

-limiting both local and remote access to the hypervisor.

The virtual network between the hypervisor and the VM is also a potential attack surface.

Responsibility for security in this layer is often shared between the CSP and the customer.

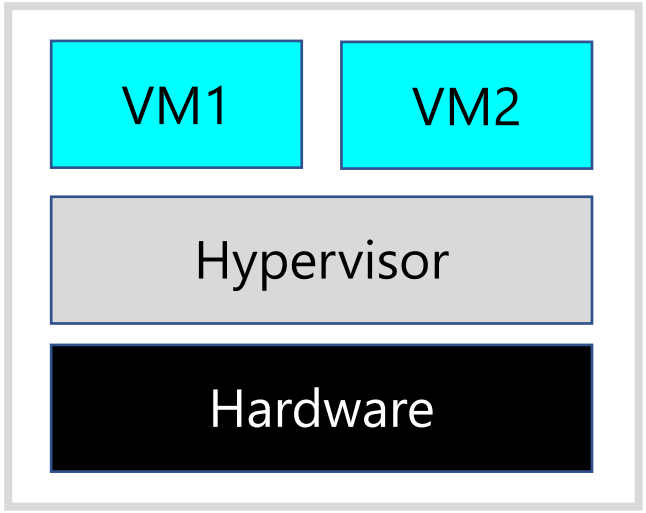
These components include virtual network, virtual switches, virtual firewalls, virtual IP addresses, etc.

Responsibility varies by model (IaaS, PaaS, SaaS)

VIRTUALIZATION RESPONSIBILITIES: **HYPERVISORS**

TYPE 1

"Bare metal"

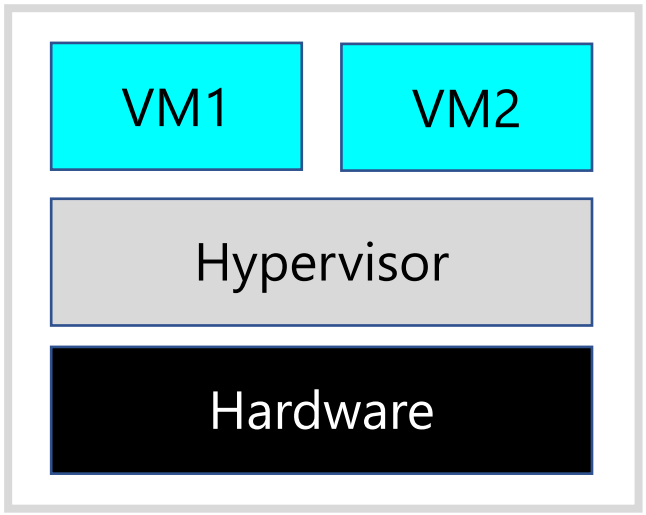


VMware ESXi, KVM
Microsoft Hyper-V

VIRTUALIZATION RESPONSIBILITIES: **HYPERVISORS**

TYPE 1

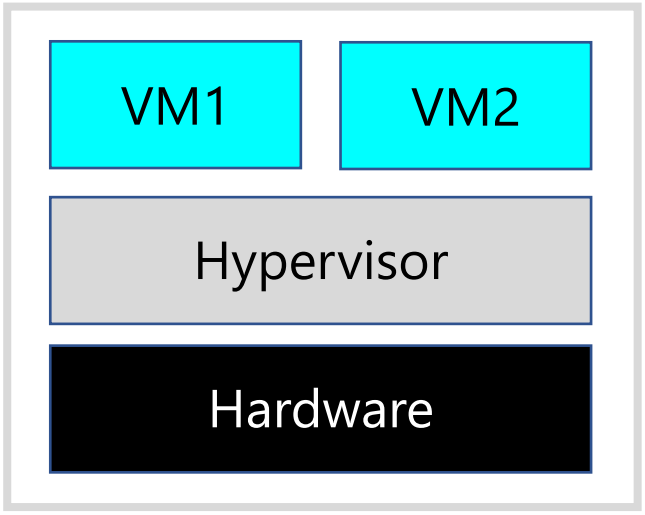
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

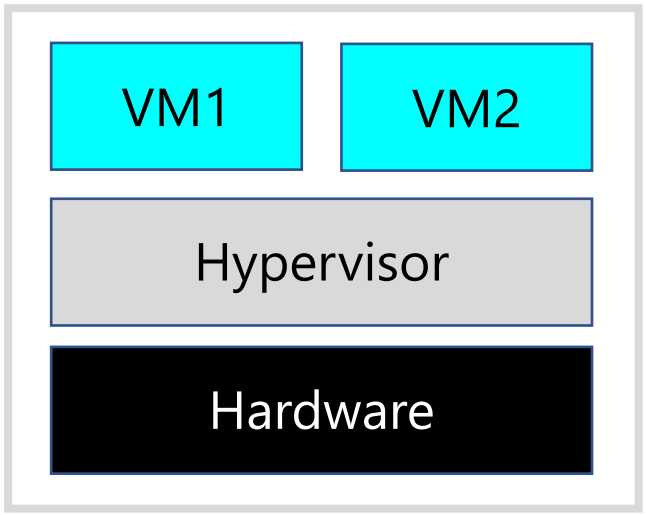
"Hosted"



VIRTUALIZATION RESPONSIBILITIES: **HYPERVISORS**

TYPE 1

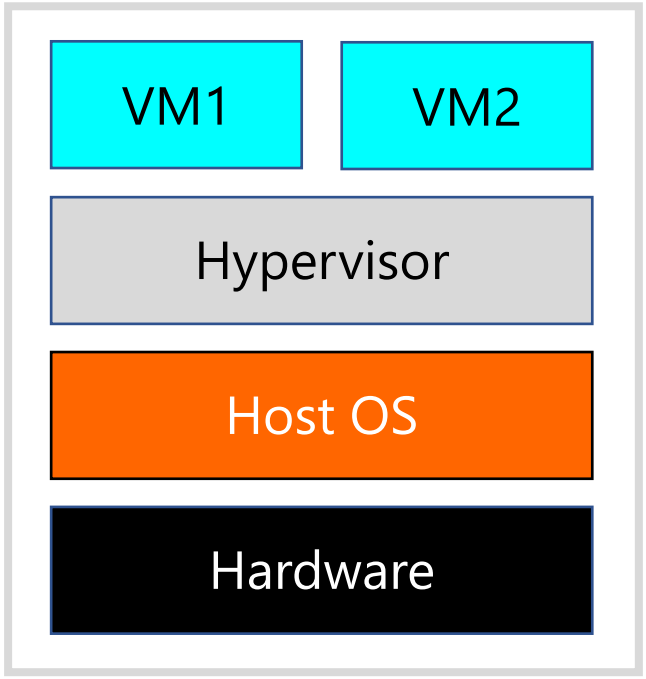
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

"Hosted"

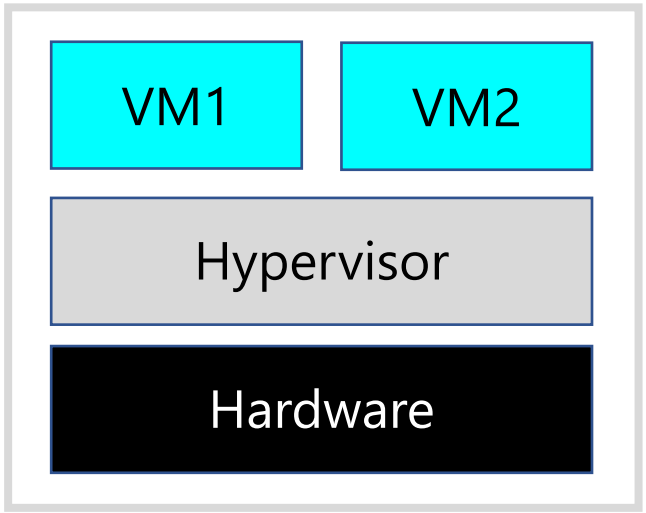


VMware Workstation,
Oracle Virtualbox

VIRTUALIZATION RESPONSIBILITIES: **HYPERVISORS**

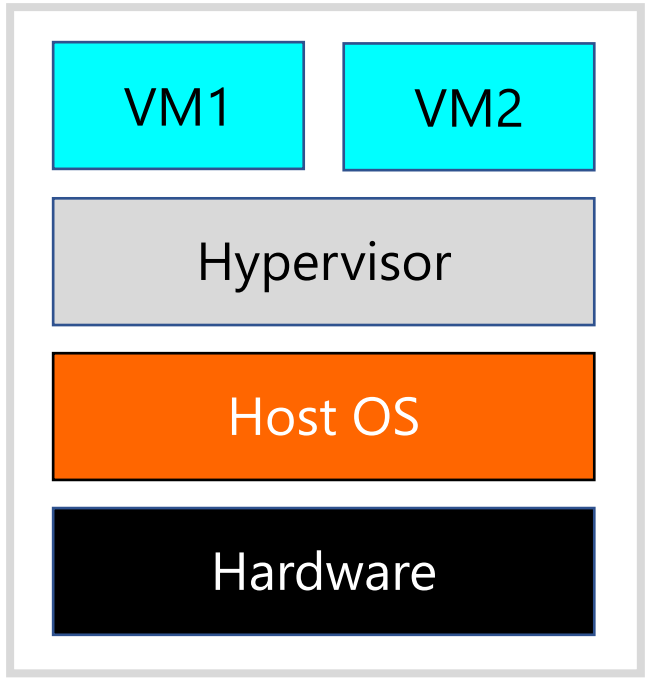
TYPE 1

"Bare metal"



TYPE 2

"Hosted"



Host hypervisor would be type 1 in nearly all cases, and the CSP is always responsible for security.

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.

or malicious user breaks the isolation between VMs running on a hypervisor by gaining access outside their VM.

Protection: Ensure patches on hypervisor and VMs are always up to date.
Ensure guest privileges are low, server-level redundancy and HIPS/HIDS protection.

STORAGE - RESPONSIBILITIES AND RISKS

Cloud storage has a number of potential security issues.

Various types of cloud storage are discussed in Domain 1

Data spends most of its life at rest, so understanding who is responsible for securing cloud storage is key.

CSP Responsibilities

physical protection of data centers and the storage infrastructure they contain.

security patches and maintenance of underlying data storage technologies and other data services they provide

CUSTOMER Responsibilities

properly configuring and using the storage tools.

logical security and privacy of data they store in the CSP's environment.

STORAGE - CUSTOMER RESPONSIBILITIES

CSPs provide a set of controls and configuration options customers can use to secure use of their storage platforms.

Customer is responsible for:

assessing the adequacy of these controls and properly configuring and using the controls available.

Access over public Internet, VPN, or internal networks

ensuring adequate protection for the data at rest and in motion based on the capabilities offered by the CSP.

Feature configuration, key mgmt (if customer-managed)

Configuring secure access, whether private or public.

In the cloud, the customer loses control of the physical medium where data is stored but retains responsibility for data security and privacy.

STORAGE - CUSTOMER CHALLENGES & RESPONSIBILITIES

Customer challenges and responsibilities without of control of the physical medium

Inability to securely wipe physical storage and possibility of another tenant being allocated the same previously allocated storage space

Customer retains responsibility for secure deletion

Compensating controls for the lack of physical control of the storage medium include:

- only storing data in an encrypted format
- retaining control of the keys needed to decrypt the data

Together, these permit crypto-shredding when data is no longer needed, rendering any recoverable fragments useless.

MANAGEMENT PLANE

management plane control = environment control

What is the management plane?

Provides the tools (web interface and APIs) necessary to configure, monitor, and control your cloud environment.

Provides virtual management options equivalent to the physical administration options a legacy data center would provide.

e.g. powering VMs on/off, provisioning VM resources, migrating a VM

You interact with the management plane through tools including the CSP's cloud portal, PowerShell or other command line, or client SDKs

Separate from and works with the **control plane** and the **data plane**.

Control Plane and Data Plane

Control plane is what you are calling when you create top-level cloud resources with ARM & Bicep (Azure), CloudFormation (AWS) or Terraform (Infrastructure-as-Code)

Data plane performs operations on resources created through the control plane

SECURING THE MANAGEMENT PLANE

Key interfaces of the management plane

Cloud Portal. the main web interface for the CSP platform.

Azure portal, AWS Management console, Google Cloud console

Scheduling. the ability to stop/start a resource at a scheduled time.

Instance Scheduler or Lambda (AWS), Azure Automation or Functions

Orchestration. automating processes to manage resources, services, and workloads, and Infrastructure-as-Code (IaC) deployments.

CloudFormation (AWS), Azure DevOps, Cloud Build (GCP)

Maintenance. update, upgrade, security patching, etc.

Secure the management plane interfaces with multi-factor auth (MFA), role-based access control (RBAC), and role management.

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.2 Design a Secure Data Center

Logical design
(e.g., tenant partitioning, access control)

Physical design
(e.g., location, buy or build)

Environmental design
(e.g., Heating, Ventilation, and Air Conditioning (HVAC), multi-vendor pathway connectivity)

Design Resilient

LOGICAL DESIGN

The logical design of a data center is an abstraction

In the now legacy co-location (colo) scenario, customers were separated at the server rack or cage-level.

In logical data center design in the cloud, customers utilize software and services provided by the CSP.

The logical design of the cloud infrastructure should :

- create tenant partitioning or isolation
- limit and secure remote access
- monitor the cloud infrastructure
- allow for the patching and updating of systems

The CCSP exam focuses on "tenant partitioning" and "access control".

TENANT PARTITIONING

Logical isolation in CSP multitenancy makes cloud computing more affordable but create some security and privacy concerns.

If isolation between tenants is breached, customer data is at risk.

Multitenancy is a concept developed decades ago:

- business centers physically housed multiple tenants
- colocation data centers supported multiple customers

The risk in these scenarios is largely physical (server, rack, cage)

In the public cloud, tenant partitioning is largely logical.

Customers are sharing capacity across the CSP datacenter, including physical components.

CSP and tenant share responsibility for implementing and enforcing controls that address the unique multitenant risks of the public cloud.

ACCESS CONTROL

When creating a logical data center, access control is a primary concern.

A single point of access makes access control simpler and facilitates monitoring, but any single point can become a failure point as well.

Hybrid identity (single login for on-premises and cloud) can simplify identity and access management (IAM)

- One method of access control is to **federate** a customer's existing IAM system with their CSP tenant
- Another method to facilitate IAM between cloud and on-premises resources is **identity as a service (IDaaS)**

Azure Active Directory (used with Office 365) or Google's Cloud Identity (used with Google Workspace)

Local and Remote Access Controls

Remote Desktop Protocol (RDP): the native remote access protocol for Windows operating systems.

Secure Shell (SSH): the native remote access protocol for Linux operating systems, and common for remote management of network devices.

RDP and SSH both support encryption and MFA

Secure Terminal/Console-Based Access: a system for secure local access.

A KVM (keyboard video mouse) system with access controls

Jumpboxes: a bastion host at the boundary of lower and higher security zones.

CSPs offer services for this: Azure Bastion, AWS Transit Gateway

Virtual Clients: software tools that allow remote connection to a VM for use as if it is your local machine.

e.g. Virtual Desktop Infrastructure (VDI) for contractors

PHYSICAL DESIGN - BUILD VS BUY

Building your own datacenter from scratch and buying an existing facility each have their advantages and disadvantages

Build

Requires significant investment to build a robust data center

Offers the most control over datacenter design

Requires knowledge and skill to match quality of BUY option

Buy

Generally, lower cost of entry (especially in shared scenario)

Less flexibility in service design (limited to what provider offers)

Shared datacenters come with additional security challenges

CSPs offer many advantages of "build" at a "buy" price tag

PHYSICAL DESIGN – CONSIDERATIONS

One of the first considerations in datacenter design is **location**

Availability of affordable, stable, resilient electricity

Natural disaster exposure (flood, hurricane, tornado, etc.)

Availability of high-speed, redundant Internet connectivity

Availability of other utilities

Physical site security (vehicular approaches, visibility)

Location relative to existing customer datacenters (BCDR)

Geographic location relative to customers

When you move to the public cloud, most of these are CSP decisions. Customer just chooses which CSP region(s)

PHYSICAL SECURITY

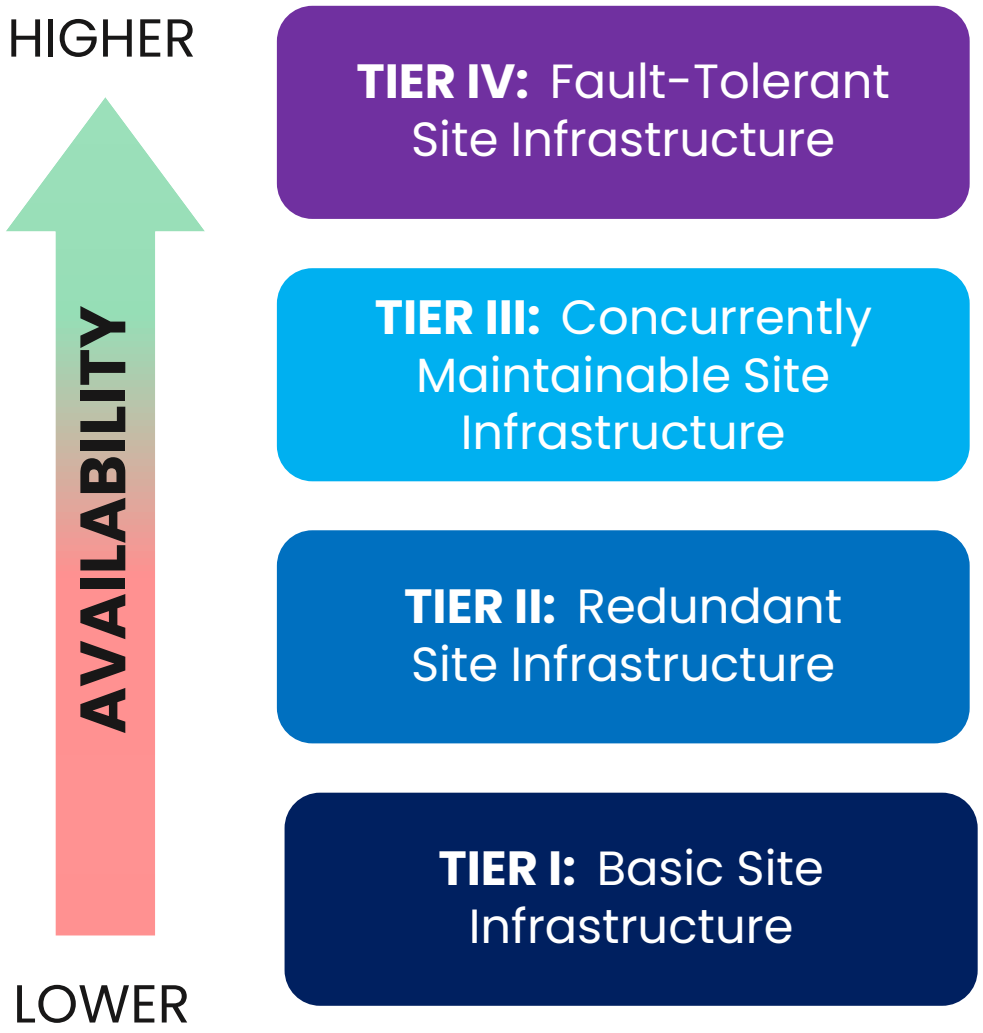
There is no security without physical security but in the cloud, this is a CSP responsibility

Know the challenges of physical security, which belong to the CSP

- A strong fence line of sufficient height and construction
- Lighting of facility perimeter and entrances
- Video monitoring and alerting
- Electronic monitoring for tampering
- Visitor access procedures with controlled entry points
- Interior access controls (badges, key codes, secured doors)
- Fire detection and prevention systems
- Protection of sensitive assets, systems, wiring closets, etc.

Due to it's cloud focus, the CCSP exam spends little time on physical security, focusing more on aspects of logical security and design.

DATACENTER TIER STANDARD



Availability and uptime are often used interchangeably, but there is a difference

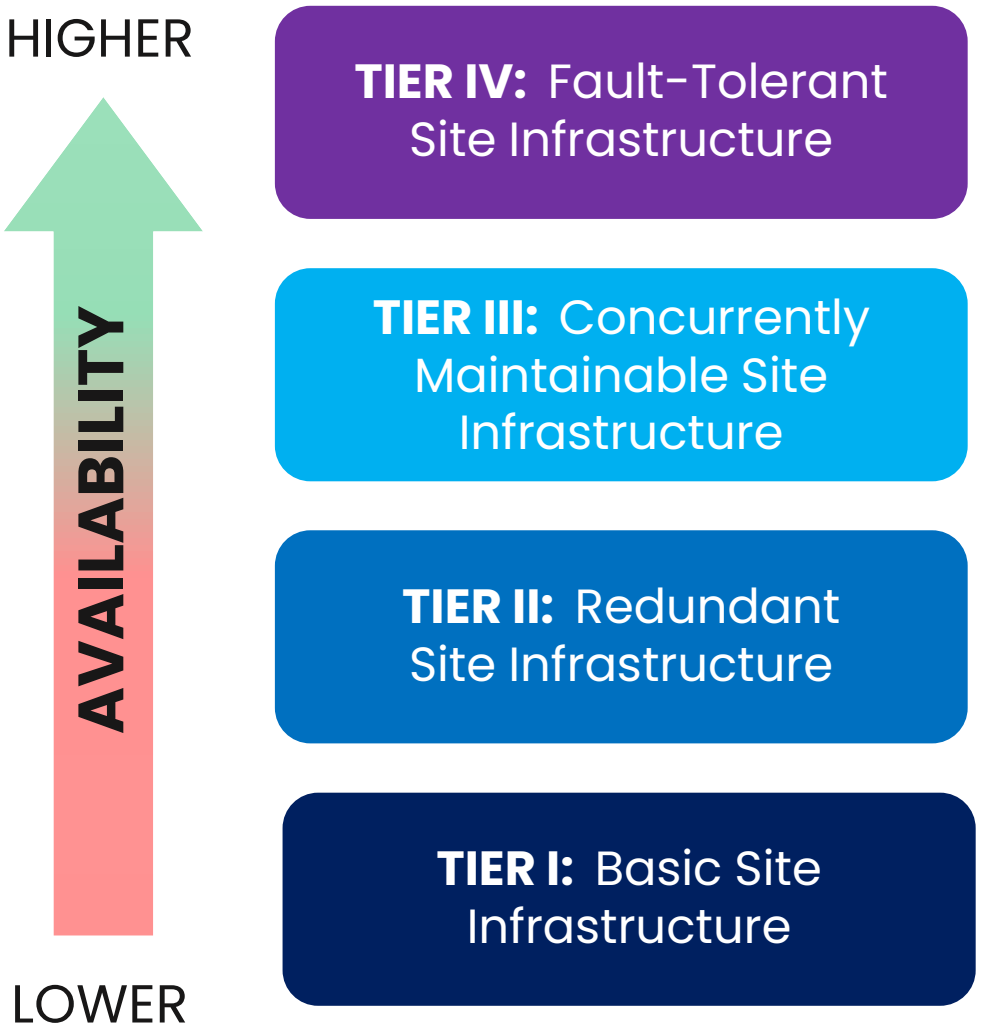
Uptime simply measures the amount of time a system is running

Availability encompasses availability of the infrastructure, applications, and services

Generally expressed as a number of 9's, such as five nines or 99.999% availability

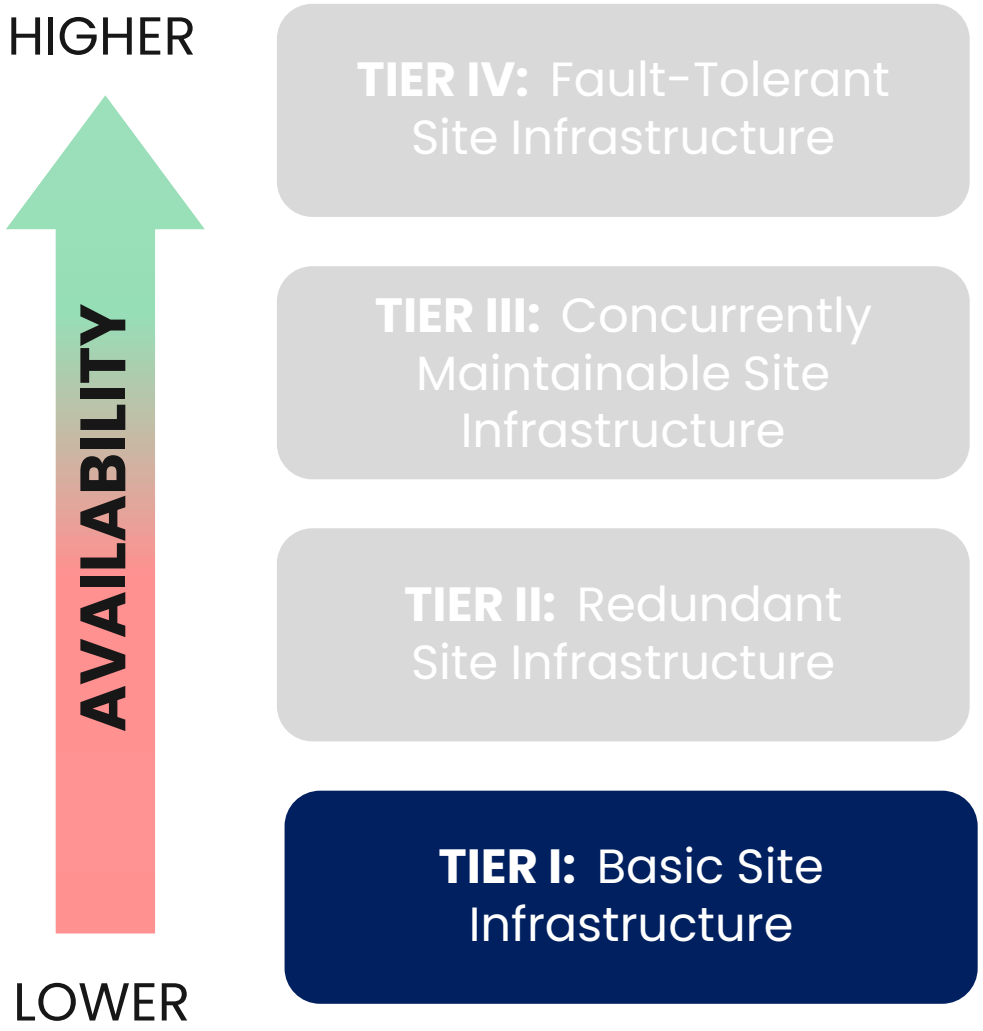
Should be measured by cloud consumer to ensure the CSP is meeting SLA obligations.

DATACENTER TIER STANDARD



The **Uptime Institute** publishes specifications for physical and environmental redundancy, expressed as tiers, that organizations can implement to achieve high availability (HA).

DATACENTER TIER STANDARD



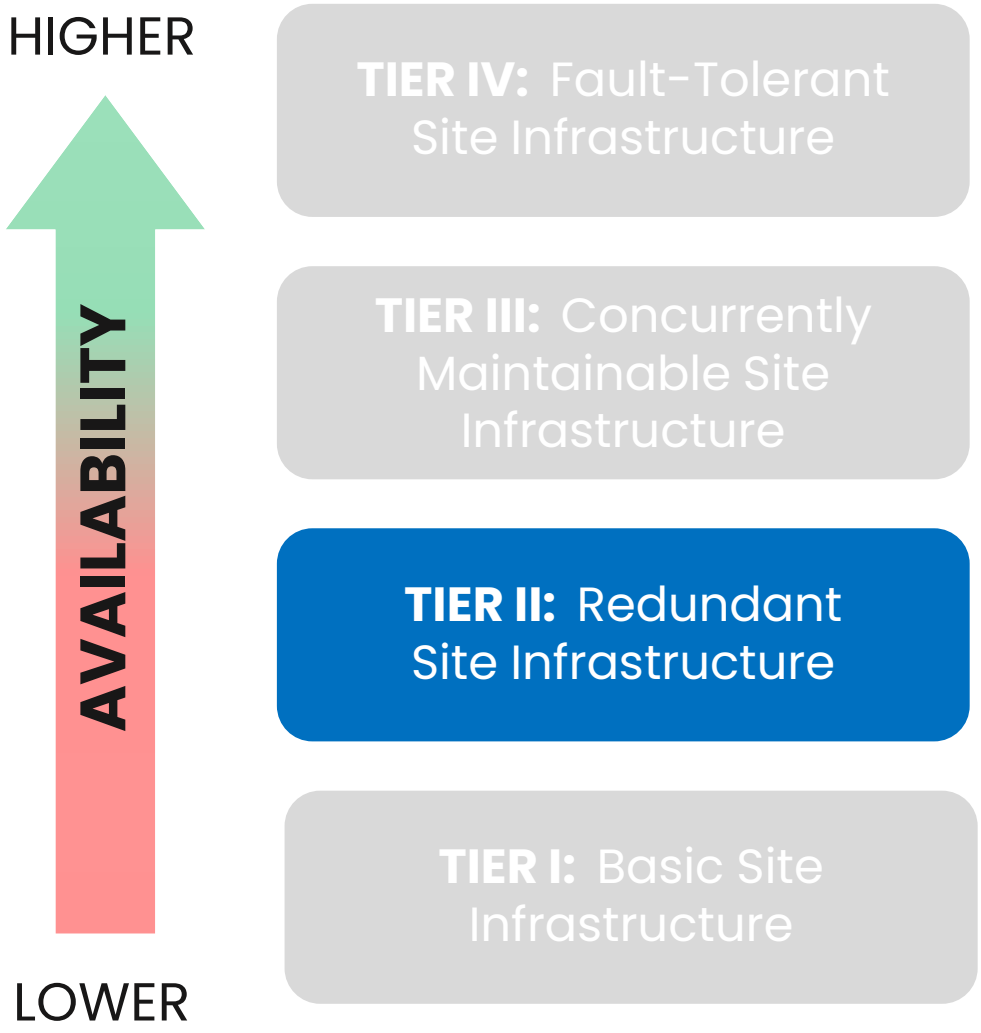
involves no redundancy and the most amount of downtime in the event of unplanned maintenance or an interruption.

must have an uninterruptible power supply that can handle brief power outages, as well as sags and spikes

must also have dedicated cooling equipment that can run on 24/7, and a generator to handle extended power outages

expected to provide 99.671% availability

DATACENTER TIER STANDARD



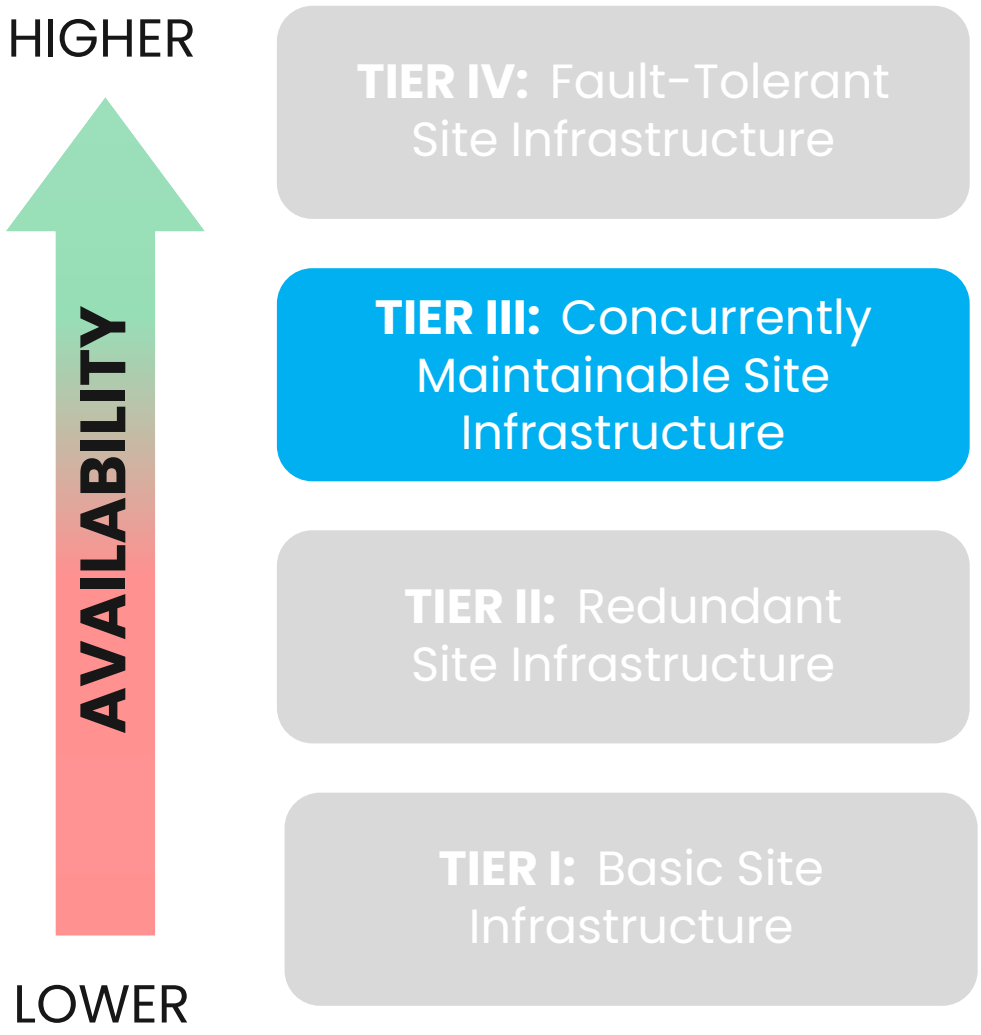
provides partial redundancy, meaning an unplanned interruption will not necessarily cause an outage

adds redundant components for important cooling and power systems

facilities must also have the ability to store additional fuel to support the generator

expected to provide 99.741% availability

DATACENTER TIER STANDARD



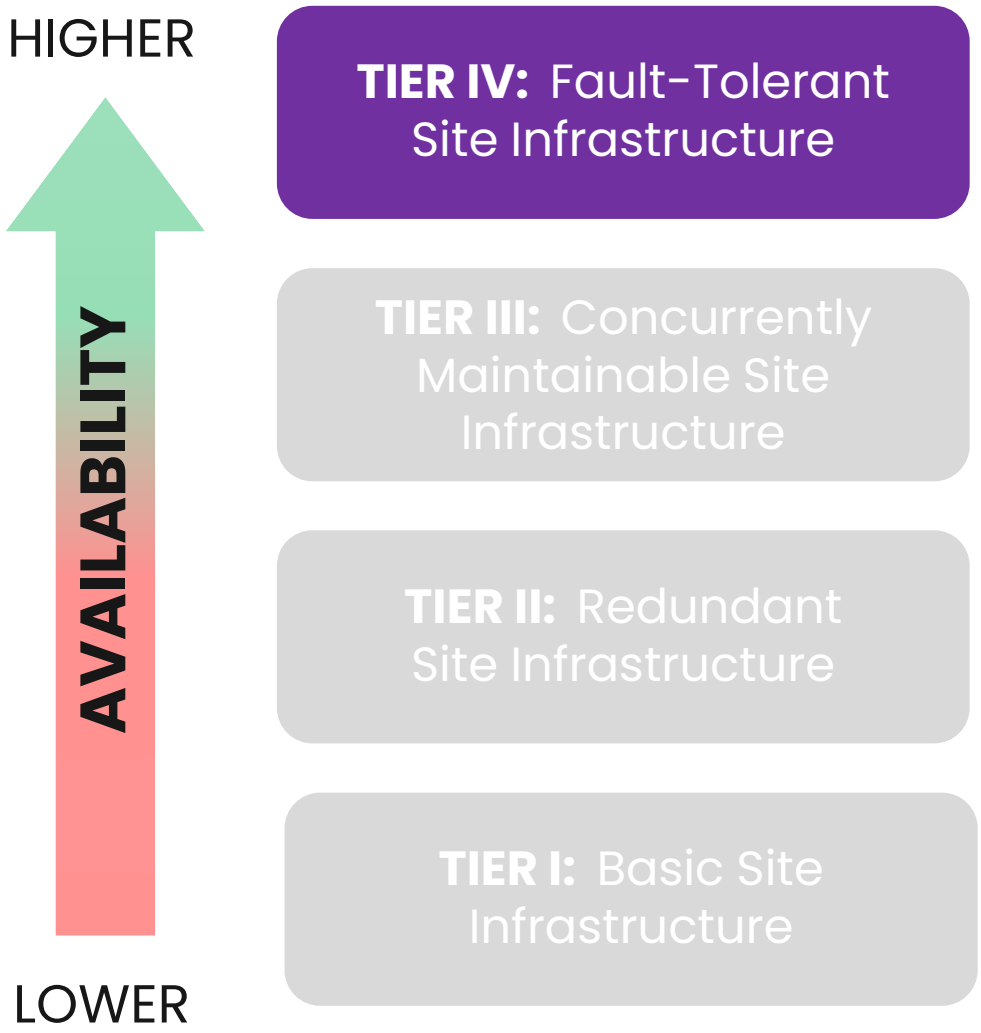
adds even more redundant components

has a major advantage in that it never needs to be shut down for maintenance

enough redundant components that any component can be taken offline for maintenance and data center continues to run

expected to provide 99.982% availability

DATACENTER TIER STANDARD



can withstand either planned or unplanned activity without affecting availability

this is achieved by eliminating all single points of failure

and requires fully redundant infrastructure, including dual commercial power feeds, dual backup generators

expected to provide 99.995% availability

HEATING, VENTILATION, AND AIR CONDITIONING

An HVAC failure can reduce availability of computing resources, just like a power failure.

Customer reviews of the CSP should include the adequacy and redundancy of HVAC systems.

A number of documents can help assess HVAC concerns, such as a SOC-2 Type II report.

Because of the confidential info in a SOC 2 Type II, some CSPs will require a nondisclosure agreement (NDA) prior to sharing.

A routine review of the most current SOC 2 report is a critical part of a cloud customer's due diligence in CSP evaluation.

WHAT IS AN SOC 2 TYPE 2 REPORT?

Statements on Standards for Attestation Engagements (SSAE)

SSAE 18 is an audit standard to enhance the quality and usefulness of System and Organization Control (SOC) reports.

designed for larger organizations, such as cloud providers (*the cost of a Type 2 report can run $30,000 or more*).

SOC-2 Type 1

report that assesses the design of security processes at a specific point in time.

SOC-2 Type 2 ←

(often written as "Type II") assesses how effective those controls are over time by observing operations for six months.

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Retrieving a SOC-2 Type II report from a CSP

EXAMPLE FOR CONTEXT:
Process will vary by CSP

INSIDE CLOUD AND SECURITY

MULTIVENDOR PATHWAY CONNECTIVITY

Protects availability

Connectivity to data center locations from more than one internet service provider (ISP) is **multi-vendor pathway connectivity**

Using multiple vendors is a proactive way for CSPs to mitigate the risk of losing network connectivity.

Best practice for CSPs or data centers is dual-entry, dual-provider for high availability:

Two providers, entering the building from separate locations

Cloud customers should consider multiple paths for communicating with their cloud vendor.

Design Resilient

Resilient designs are engineered to respond positively to changes or disturbances, such as natural disasters or man-made disturbances.

DESIGN RESILIENT

A few examples of resilient design:

- ✓ HA firewalls, active-passive or active-active
- ✓ Multi-vendor pathway connectivity
- ✓ Web server farm (behind redundant load balancers)
- ✓ Database cluster (Windows / Linux cluster feature)

Service-level resiliency requires identifying single points of failure throughout the service chain

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.3 Analyze Risks Associated with Cloud Infrastructure and Platforms

Risk assessment
(e.g., identification, analysis)

Cloud vulnerabilities, threats and attacks

Risk mitigation strategies

RISK ASSESSMENT, IDENTIFICATION, AND ANALYSIS

The **risk management process** is fundamental to information security, since the entire practice involves **mitigating and managing risks** to data and information systems.

Careful selection of CSPs and the development of SLAs and other contractual agreements are critical to mitigating risk

Organizations can balance cost savings with risk by building a system on top of IaaS or PaaS, rather than utilizing a SaaS solution.

IaaS means more control, more responsibilities, and risks

and confirming their CSP does the same!

Customers must be proactive in addressing their responsibilities under the shared responsibility model.

RISK ASSESSMENT - IDENTIFICATION

Identifying risks is the first step in managing them and begins with identification of the organization's valuable assets

Once assets are identified:

Security practitioners and risk managers can then begin to identify potential causes of disruption to the assets.

RISK FRAMEWORKS

Several exist that provide processes and procedures for designing and implementing a risk management framework.

- **ISO/IEC 31000:2018**, *Risk Management Guidelines*
- **NIST SP 800-37**, *Guide for Applying the Risk Management Framework to Federal Information Systems*

QUANTITATIVE RISK ASSESSMENT

Assigns a **dollar value** to evaluate effectiveness of countermeasures

Objective, ensure controls are cost effective

RISK ASSESSMENT - IDENTIFICATION

Risks specific to cloud environments should be identified when making the decision to use a cloud service.

RISK ASSESSMENT - ANALYSIS

Analyzing identified risks continues the conversation started by "What could go wrong?"

Analysis seeks to answer two questions:

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $

How likely is it to happen?

Annualized Rate of Occurrence (ARO) - decimal

An impact that happens *twice a year* has an ARO of **2.0**
An impact that happens *once every two years* has an ARO of **0.5**
An impact that happens *once every five years* has an ARO of **0.2**

RISK ASSESSMENT - ANALYSIS

Analyzing identified risks continues the conversation started by "What could go wrong?"

Analysis seeks to answer two questions:

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $

How likely is it to happen?

Annualized Rate of Occurrence (ARO) - decimal

With these two figures, we can determine our **annualized loss expectancy (ALE)**

Annualized Loss Expectancy (ALE)

The possible yearly cost of all instances of a specific realized threat against a specific asset.

RISK ASSESSMENT - ANALYSIS

Analyzing identified risks continues the conversation started by "What could go wrong?"

Analysis seeks to answer two questions:

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $

How likely is it to happen?

Annualized Rate of Occurrence (ARO) - decimal

FORMULA

ALE = SLE x ARO

RISK ASSESSMENT - ANALYSIS

SCENARIO: It is estimated a tornado may strike a branch office once every 5 years, causing 30% loss to a $1,000,000 building.

Calculating the cost of a single occurrence (SLE)

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $

How significant will the loss be?

Exposure factor (EF) - %

FORMULA

SLE = Asset value (AV) x EF

RISK ASSESSMENT - ANALYSIS

SCENARIO: It is estimated a tornado may strike a branch office once every 5 years, causing 30% loss to a $1,000,000 building.

Calculating the cost of a single occurrence (SLE)

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $

How significant will the loss be?

Exposure factor (EF) - %

EXAMPLE

$1,000,000 Building X 0.30 Expected loss (our EF) = $300,000 Single loss expectancy (SLE)

RISK ASSESSMENT - ANALYSIS

SCENARIO: It is estimated a tornado may strike a branch office once every 5 years, causing 30% loss to a $1,000,000 building.

Calculating the cost of annualized cost (ALE)

What will the impact be if that goes wrong?

Single loss expectancy (SLE) - $300,000

How likely is it to happen?

Annualized rate of occurrence (ARO) - 0.2

EXAMPLE

$300,000
Single loss expectancy (SLE)

X 0.2
Annualized rate of occurrence

= $60,000
Annualized loss expectancy (ALE)

Analysis of CSP Risks

Analysis of a CSP or cloud solution and the associated risks involves many departments and focus areas:

- Business units
- Vendor management
- Privacy
- Information security

CSP operations should also be considered, but most major CSPs are audited for ISO/IEC 27001, 27017,27018

Analysis of CSP Risks

There are standards to guide CSPs in their preparation or customer evaluation of cloud service providers.

ISO/IEC 27001

a framework for policies and procedures that include legal, physical, and technical controls involved in an organization's information risk management processes.

ISO/IEC 27017

Covered in depth in Domain 1 (section 1.5)

a security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.

ISO/IEC 27018

Will be covered in depth in Doman 6 (section 6.2)

the first international standard about the privacy in cloud computing services

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Validating CSP compliance with ISO/IEC 27001, 27017, & 27018

EXAMPLE FOR CONTEXT:
Location will vary by CSP

INSIDE CLOUD AND SECURITY

Analysis of CSP Risks

Risks with a cloud solution are mainly associated with data privacy and information security:

Authentication Risk

Does the CSP provide a solution or is this a customer responsibility?

Customer-managed or CSP-managed?

Data Security

How a vendor encrypts data at rest, strength of the cryptography, and access controls that prevent unauthorized access by cloud service personnel or other tenants.

Some controls on by default, customer may have to enable others

Analysis of CSP Risks

Risks with a cloud solution are mainly associated with data privacy and information security:

Supply Chain Risk Management (SCRM)
Evaluation of vendor security policies and processes.

Most CSPs do not allow direct auditing of their operations, due to the number of customers they support.

Instead, they provide standardized reports and assurance material regarding their security practices, such as

- SOC 2 report
- ISO 27001 certification
- Specialized reports for regulated data

→ HIPPA, FedRAMP, ISO/IEC 27017, 27018

Common Cloud Risks

One risk that has been discussed is the organization losing ownership and full control over system hardware assets.

Careful selection of CSPs and the development of SLAs and other contractual agreements are critical to limiting risk

Organizations can balance cost savings with risk by building a system on top of IaaS or PaaS, rather than utilizing a SaaS solution.

REMEMBER: The service model affects the level of control!

Regardless of which deployment or service model is used, some risks are common to all cloud computing environments.

Common Cloud Risks

Geographic dispersion of the CSP data centers
If the cloud service is properly architected, a disruption at one data center should not cause a complete outage.

Customers must verify the resilience and continuity controls in place at the CSP

Downtime
Resilience for network disruptions can be built in multiple ways, such as multivendor connectivity, zones and regions.

Discussed in 'cloud shared considerations' in Domain 1

Common Cloud Risks

Compliance
Privacy data in some jurisdictions cannot be transferred to other countries, so data dispersion is inappropriate.

Major CSPs have compliance-focused service offerings

General technology risk
Cloud systems are not immune to standard security issues like cyberattacks.

CSP defenses should be documented and tested, and customers aware of their configuration responsibilities

RISK TYPES

External

Different threat actors, ranging from competitors and script kiddies to criminal syndicates and state actors.

Capabilities depend on tools, experience, and funding.

Other external environmental threats, such as fire and floods, and man-made threats, such as the accidental deletion of data or users.

Internal

A malicious insider, a threat actor who may be a dissatisfied employee (someone overlooked for a promotion).

Another internal threat is human error, which is when data is accidentally deleted.

Customer should know who is responsible for configuration

CSPs also face these risks. Customers should verify their CSP has addressed them or provided tools to help customers

CLOUD VULNERABILITIES, THREATS AND ATTACKS

The primary vulnerability in the cloud is that it is an Internet-based model

Organizations could be at risk if the CSP's public-facing infrastructure comes under attack

Any attack on your CSP or cloud vendor may be unrelated to you as an organization

Threat actors may be targeting the CSP or another tenant of the CSP

Risks can come from the other tenants as well.

Customers may be "collateral damage" of an attack on the CSP!

CLOUD VULNERABILITIES, THREATS AND ATTACKS

Cloud-Specific Risks

The Cloud Security Alliance details the top cloud-specific security threats in their list titled "**The CSA Egregious 11**"

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. "Metastructure" and "applistructure" failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

The "CSA Egregious 11"

Data breaches Unintentional loss/oversharing is a "data leak"
Loss of sensitive data (PII, PHI, intellectual property) due to security breach.

Misconfiguration and inadequate change control
Software can offer the most secure configuration options, but if it is not properly set up, then the resulting system will have security issues.

Remediate risk through change and configuration management

Lack of cloud security, architecture, and strategy
As organizations migrate to the cloud, some overlook security, or fail to consider their obligations in the shared responsibility model.

Insufficient identity, credential access, and key management
The public cloud offers benefits over legacy on-premises environments but can also bring additional complexities.

Well-architected identity and access management (IAM), encryption, secret and key management are different than on-prem and essential

The "CSA Egregious 11"

Account hijacking ← Phishing is the most common approach
Credential theft, abuse, and/or elevation to carry out an attack.

Insider threat
Disgruntled employees, employee mistakes, and unintentional over-sharing.
Job rotation, privileged access management, auditing, security training

Insecure interfaces and APIs
Customers failing to secure access to systems gated by APIs, web consoles, etc.
Controls include MFA, RBAC, and key-based API access

Weak control plane
Weaknesses in the elements of a cloud system that enable cloud environment configuration and management (web console, CLI, and APIs)
Most CSPs offer reference architectures to ensure customers secure and isolate their dev/test/prod environments and data

CCSP

CSSP EXAM CRAM
THE COMPLETE COURSE

DEMO

Insider threat protections offered by CSPs

EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

INSIDE CLOUD AND SECURITY

The "CSA Egregious 11"

Metastructure and applistructure failures
Vulnerabilities in the operational capabilities that CSPs make available, like APIs for accessing various cloud services.

If the CSP has inadequately secured these interfaces, any resulting solutions built on top of those services will inherit these weaknesses.

Metastructure. The protocols and mechanisms that provide the interface between the cloud layers, enabling management and configuration.

Applistructure. Applications deployed in the cloud and the underlying application services used to build them.

e.g. PaaS features like message queues, functions, and message services

Responsibility? Mitigation?
Mitigating risks in this area is the responsibility of the CSP. Customers should verify the CSP has implemented their own SSDLC to ensure service security.

The "CSA Egregious 11"

Limited cloud usage visibility

Refers to when organizations experience a significant reduction in visibility over their information technology stack.

This is because in some models, the CSP own the stack!

Abuse and nefarious use of cloud services

While the low cost and high scale of compute in the cloud is an advantage to enterprises, it is an opportunity for attackers to execute disruptive attacks at scale.

Makes executing DDoS and phishing attacks easier, so CSPs must implement mitigating security controls for these risks

RISK MITIGATION STRATEGIES

There are several approaches to risk mitigation in cloud environments.

Selecting a qualified CSP is an essential first step.

The next step is designing and architecting with security in mind.

Security should be considered at every step starting with design!

The next risk mitigation tool is encryption, and data should be encrypted at rest and in-transit.

Storage and database encryption at rest, TLS and VPN in-transit

Finally, ongoing monitoring and management to maintain posture.

Major CSPs provide the ability to manage and monitor configuration security, and to monitor changes to cloud services, and track usage

CSSP EXAM CRAM
THE COMPLETE COURSE

DEMO

Ongoing monitoring to maintain security posture

EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

INSIDE CLOUD AND SECURITY

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.4 Design and Plan Security Controls

Physical and environmental protection
(e.g. on-premises)

System, storage and communication protection

Identification, authentication and authorization in cloud environments

Audit mechanisms
(e.g. log collection, correlation, packet capture)

PHYSICAL AND ENVIRONMENTAL PROTECTION

The primary consideration is the **site location**, as it will have an impact on both physical and environmental protections.

Cloud data centers share requirements with traditional colocation providers or individual data centers, including:

- ability to **restrict physical access** at multiple points
- ensuring a clean and stable **power supply**
- adequate **utilities** like water and sewer
- the availability of an adequate **workforce**

These are customer responsibilities in on-premises (private) cloud, and CSP responsibility in the public cloud

PHYSICAL AND ENVIRONMENTAL PROTECTION

The primary consideration is the **site location**, as it will have an impact on both physical and environmental protections.

Cloud data centers share requirements with traditional colocation providers or individual data centers, including:

- ability to **restrict physical access** at multiple points
- ensuring a clean and stable **power supply**
- adequate **utilities** like water and sewer
- the availability of an adequate **workforce**

Expect less exam focus on physical considerations since it's a CSP area of responsibility for public cloud

SITE SELECTION & FACILITY DESIGN

Key elements in **site selection** and **facility design**.

For site selection

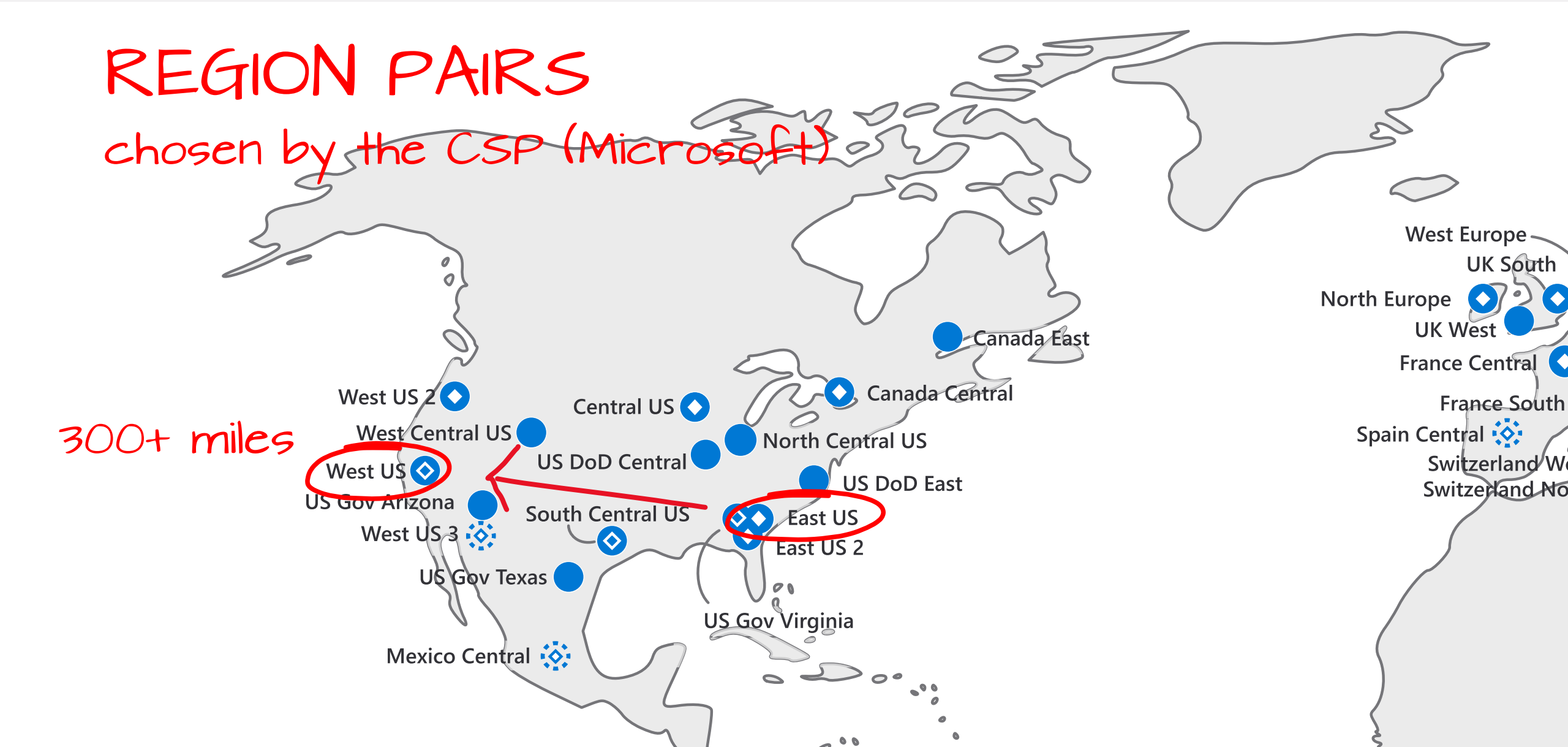
Visibility, composition of the surrounding area, area accessibility, and the effects of natural disasters.

These are all problems for the CSP in public cloud

Customers should focus on selecting CSP datacenter locations to meet disaster recovery and data residency

Remember CSPs auto-select region pairs for redundancy!

SITE SELECTION



SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

System and Communication Protection

Technology

Encrypt and protect data:

- ✓ at rest
- ✓ in transit
- ✓ in use

Protect systems and services:

- ✓ DoS/DDoS
- ✓ Boundary (ingress and egress)
- ✓ Key Management

Security practices

People and processes

- ✓ Automation of configuration
- ✓ Responsibilities for protecting cloud systems and services
- ✓ Monitoring and maintenance

Customer and CSP roles vary based on the "Shared Responsibility Model"

SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

Properly securing information systems can be a difficult task due to the sheer number of elements that make up a system.

Breaking systems down into components and then applying security controls can make the overall task more manageable.

One source for controls is **NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"**, which contains a family of controls specific to systems and communications

The NIST control family includes 50+ controls, many relevant to system, storage, and communication protection

SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

Properly securing information systems can be a difficult task due to the sheer number of elements that make up a system.

- Policy and Procedures
- Separation of System and User Functionality
- Security Function Isolation
- Denial-of-Service Protection
- Boundary Protection
- Cryptographic Key Establishment and Management

SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

Policy and Procedures

Establish requirements for system protection, and define the purpose, scope, roles, and responsibilities needed to achieve it.

Separation of System and User Functionality

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

Separating user and admin functions can also prevent users from altering processes or misconfiguring systems.

Security Function Isolation

Separating security-specific functions from other roles is another example of separation of duties.

e.g. configuring data security controls like encryption and logging configuration

SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

Denial-of-Service Protection

A disruptive attack at scale that is more difficult for smaller organizations to combat effectively.

Most CSPs offer DoS/DDoS mitigation as a service, and there are also dedicated providers like Akamai and Cloudflare.

e.g. Azure DDoS, AWS Shield, Google Cloud Armor

Boundary Protection

Deals with both ingress and egress protections, including:

- ✓ Preventing malicious traffic from entering the network
- ✓ Preventing malicious traffic from leaving your network
- ✓ Protecting against data loss (exfiltration)
- ✓ Configuring rules/policies in routers, gateways, or firewalls

SYSTEM, STORAGE, AND COMMUNICATION PROTECTION

Cryptographic Key Establishment and Management

Cryptography provides a number of security functions including confidentiality, integrity, and nonrepudiation.

Encryption tools like TLS or a VPN can be used to provide confidentiality.

Hashing can be implemented to detect unintentional data modifications. integrity

Additional security measures like **digital signatures** or hash-based message authentication code (HMAC) can be used to detect intentional tampering.

HMAC can simultaneously verify both data integrity and message authenticity

IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

AuthN and AuthZ

Identity

Authentication (AuthN) is the process of proving that you are who you say you are.

Authorization (AuthZ) is the act of granting an authenticated party permission to do something.

Access

IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

AuthN and AuthZ

Permissions, **rights**, and **privileges** are granted to users based on their proven identity.

If user has assigned rights to a resource, they are granted **authorization**.

Users should be granted minimum necessary permissions.
This is the principle of least privilege.

ACCOUNTABILITY

Users who perform activities on a system are held accountable for following policies and procedures

Accountability is typically enforced with adequate logging and monitoring of system activity

Cloud challenges in enforcing accountability

- SaaS apps used as users travel make identifying anomalous / malicious behavior more difficult
- Bad password practices (reuse across services)
- Use of personal devices in BYOD scenarios

Modern IDaaS tools provide solutions for these challenges

MULTIFACTOR AUTHENTICATION (MFA)

MFA

MFA works by requiring two or more of the following authentication methods:

MFA FACTORS AND ATTRIBUTES

MFA

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

Something you **have** (trusted device)

Something you **are** (biometric)

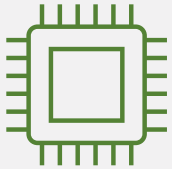
Software OATH

Time-based one-time passwords (TOTP)

Authenticator app

Voice call

SMS (text msg)



OATH HW token

MFA FACTORS AND ATTRIBUTES

Multifactor Authentication

includes two or more authentication factors

more secure than using a single authentication factor

passwords are the weakest form of authentication

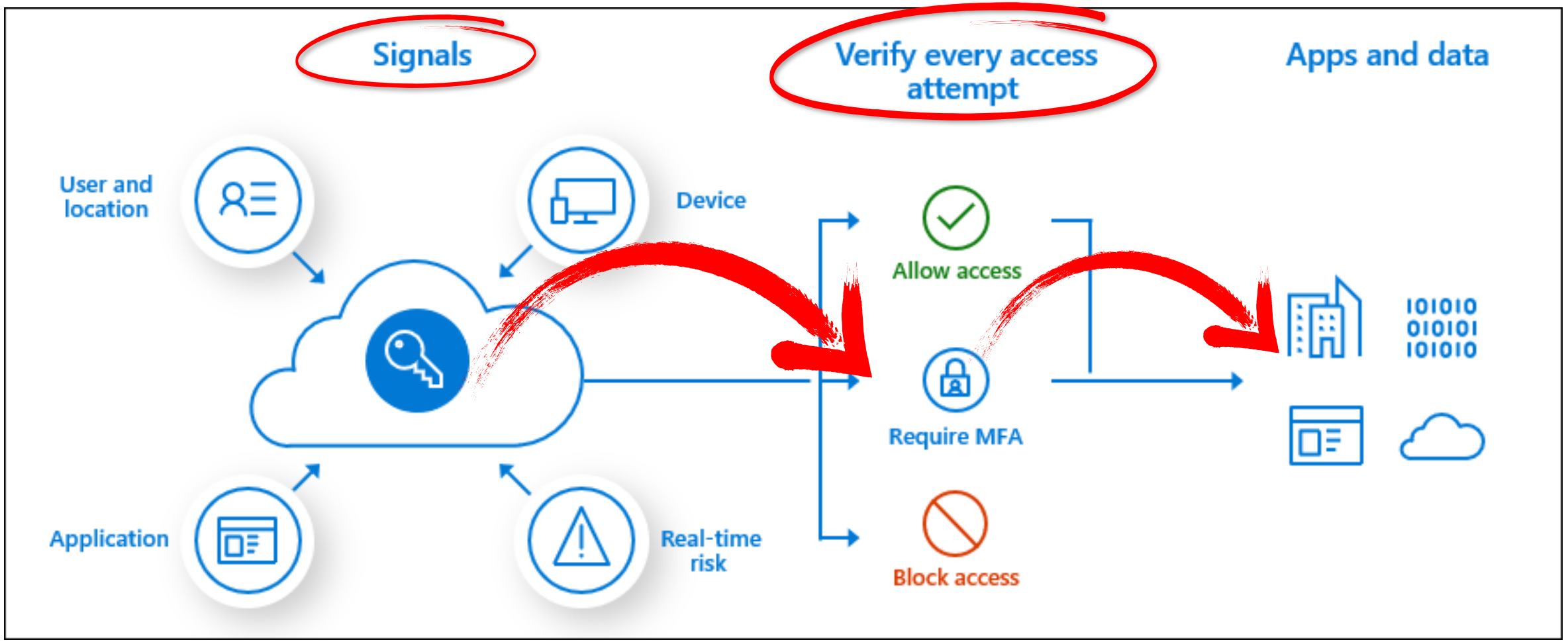
password policies help increase their security by enforcing complexity and history requirements

Smartcards include microprocessors and cryptographic certificates

Oath tokens create one-time passwords (OTP)

Biometric methods identify users based on individual characteristics such as fingerprints and facial recognition

CONDITIONAL AUTHENTICATION POLICIES



signal > decision > enforcement

image credit: Microsoft

AUTHENTICATION METHODS

Authentication applications

"Authenticator apps"

is a software-based authenticator that implements two-step verification services using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm, for authenticating users of software applications.

Examples include Microsoft Authenticator and Google Authenticator.

Authenticator apps from companies like Microsoft and Google generate one-time passcodes using open standards developed by the **Initiative for Open Authentication (OATH)**. You'll hear HMAC and TOTP tokens called OATH tokens with some of these providers.

Push notifications

where the server is pushing down the authentication information to your mobile device.

uses the mobile device app to be able to receive the pushed message and display the authentication information.

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Conditional authentication policies in Identity-aaS

EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

INSIDE CLOUD AND SECURITY

DESCRIBE THE CONCEPT OF FEDERATED SERVICES

Federation is a collection of domains that have **established trust.**

The level of trust may vary, but typically includes authentication and almost always includes authorization.

Often includes a number of organizations that have established trust for shared access to a set of resources.

Example

You can federate your on-premises environment with Azure Active Directory (Azure AD) and use this federation for authentication and authorization.

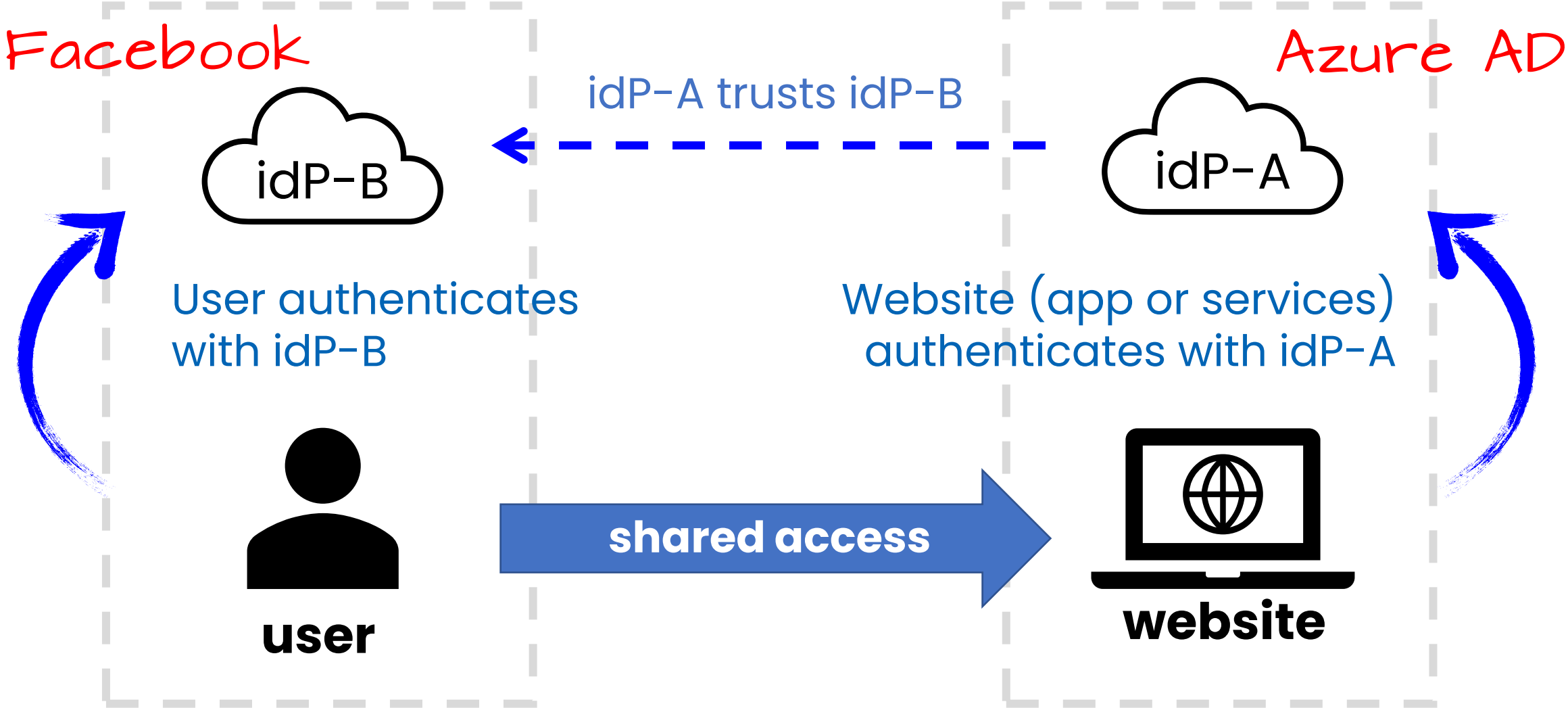
This sign-in method ensures that all user authentication occurs on-premises.

Allows administrators to implement more rigorous levels of access control.

Certificate authentication, key fob, card token

IDENTITY FEDERATION (EXAMPLE)

may be cloud or on-premises



trust is not always bi-directional

AUDIT MECHANISMS

Log Collection

Cloud services will offer different controls over what information is logged…

but at a minimum level of security-relevant events, such as use of or changes to privileged accounts

A log aggregator can ingest logs from all on-premises and cloud resources for review.

Both were discussed in Domain 2

NIST SP 800-53 and the **OWASP logging cheat sheet** offer guidance on specific information to capture in audit records.

Correlation

Refers to the ability to discover relationships between two or more events across logs.

This capability is commonly associated with a SIEM, which correlates events in logs from many sources

PACKET CAPTURE AND REPLAY

Packet capture tools are also called **protocol analyzers**

The cloud environment may not provide any facility for capturing packets, particularly in SaaS scenarios

Wireshark: a free, open-source protocol analyzer, with CLI and GUI versions, available for Windows and Linux.

Some CSPs support Wireshark, others have specialized services to perform packet capture on virtual networks.

e.g. Network Watcher (Azure), AWS supports Wireshark

Some CSP protocol analyzers can save the data that they collect to a Wireshark-compatible packet capture file (PCAP).

3. CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

3.5 Plan Disaster Recovery (DR) and Business Continuity (BC)

Business continuity (BC) / disaster recovery (DR) strategy

Business requirements
(e.g. Recovery Time Objective (RTO), Recovery Point Objective (RPO), recovery service level)

Creation, implementation and testing of plan

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

GOALS OF DRP AND BCP

What are the core goals of disaster recovery and business continuity planning?

Minimizing the effects of a disaster by:

Improving responsiveness by the employees in different situations.

Easing confusion by providing written procedures and participation in drills

Helping **make logical decisions** during a crisis

BCP DEFINITIONS

Some BCP-related definitions worth knowing

BRP (Business Resumption Plan)
the plan to move from the disaster recovery site back to your business environment or back to normal operations.

MTBF (Mean Time Between Failures)
a time determination for how long a piece of IT infrastructure will continue to work before it fails.

MTTR (Mean Time to Repair)
a time determination for how long it will take to get a piece of hardware/software repaired and back on-line.

BCP DEFINITIONS

Some BCP-related definitions worth knowing

MTD (Max tolerable downtime)

The amount of time we can be without the asset that is unavailable BEFORE we must declare a disaster and initiate our disaster recovery plan.

BCDR STRATEGY

Important BCP-related definitions for the exam

BCP (Business Continuity Plan) Business-focused

The overall organizational plan for "how-to" continue business after an event has occurred.

A proactive risk mitigation strategy that contains likely scenarios that could affect the organization and guidance on how the organization should respond

Sometimes called a continuity of operations plan (COOP)

DRP (Disaster Recovery Plan) Tech-focused

the plan for recovering from an IT disaster and having the IT infrastructure back in operation.

BUSINESS IMPACT ANALYSIS

The **business impact assessment (BIA)** is used to determine which processes are critical and which are not.

Measures the impact of specific systems and processes.

Any that are deemed critical to the organization's functioning must be prioritized in an emergency situation.

A BIA typically contains a **cost-benefit analysis (CBA)** and a calculation of the **return on investment (ROI)**.

BCP/DRP FROM A CSP PERSPECTIVE

A cloud data center that is affected by a natural disaster will likely activate multiple BCPs and DRPs.

CSP will activate both plans to deal with the interruption to their service.

One key element of the BCP is communicating incident status to relevant parties.

BCP/DRP FROM A CUSTOMER PERSPECTIVE

The **customer is responsible** for determining how to recover in the case of a disaster in the cloud.

Customer may choose to implement backups, or utilize multiple availability zones, load balancers, or other techniques.

CSPs can further protect customers by not allowing two availability zones within a single physical datacenter within a cloud region.

Let's revisit the concept of availability zones in a cloud datacenter (covered in Domain 1)

DESCRIBE CORE ARCHITECTURE COMPONENTS

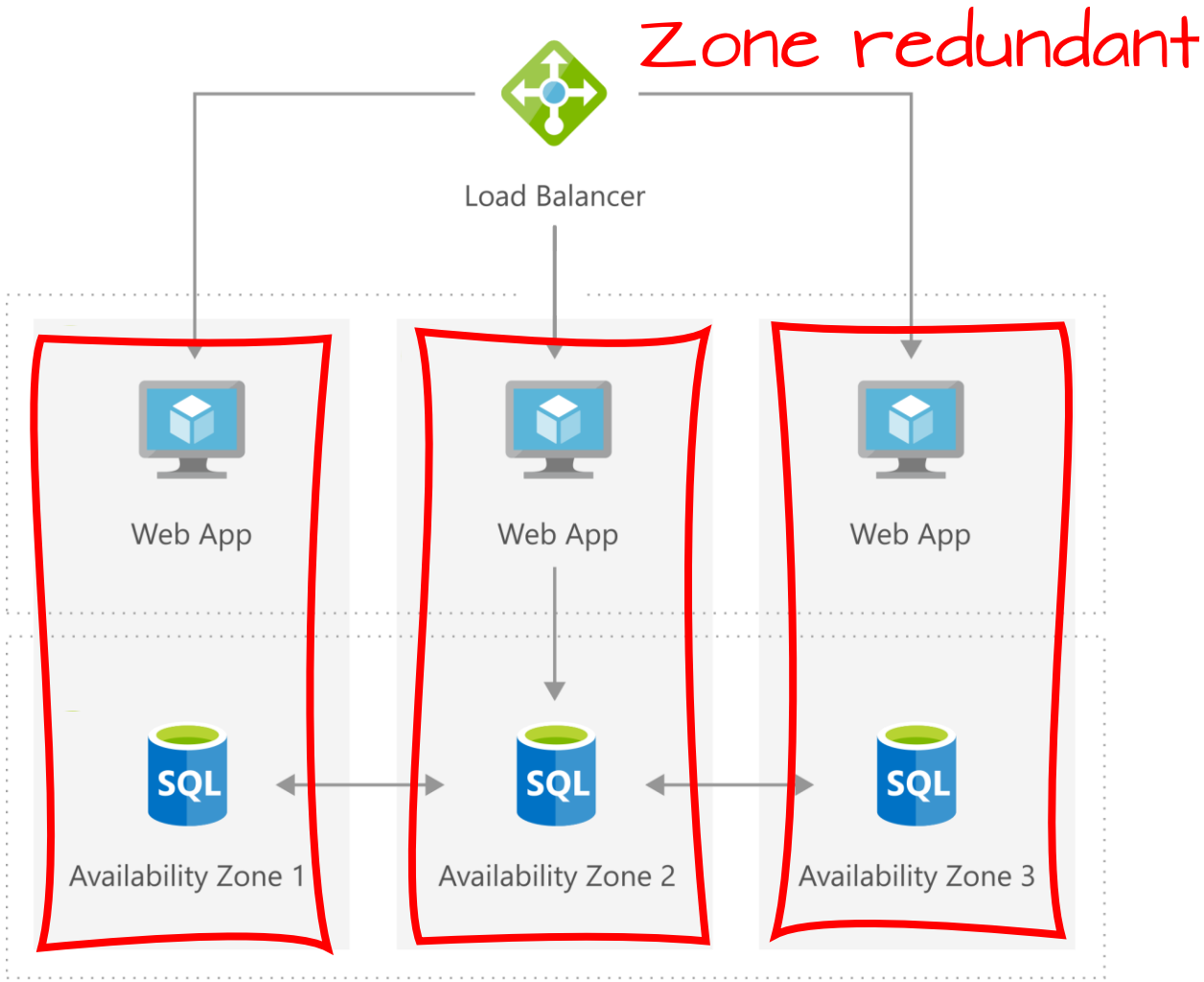
Availability Zones

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



BCP/DRP FROM A CUSTOMER PERSPECTIVE

The **customer is responsible** for determining how to recover in the case of a disaster in the cloud.

Customer may choose to implement backups, or utilize multiple availability zones, load balancers, or other techniques.

CSPs can further protect customers by not allowing two availability zones within a single physical datacenter within a cloud region.

Major CSPs have multiple datacenters within a region so it can be safely assumed this is true.

Communication Plan

The plan that details how relevant stakeholders will be informed in event of an incident. (like a security breach)

Would include plan to maintain confidentiality, such as encryption to ensure that the event does not become public knowledge.

Contact list should be maintained that includes stakeholders from the government, police, customers, suppliers, and internal staff.

Compliance regulations, like GDPR, include notification requirements, relevant parties and timelines

Confidentiality amongst internal stakeholders is desirable so external stakeholders can be informed in accordance with the plan.

STAKEHOLDER MANAGEMENT

When we have an incident, there are multiple groups of relevant stakeholders that we need to inform and manage, and may include:

- Internal stakeholders
- Cyber insurance provider
- Business partners
- Customers
- Law enforcement

A **stakeholder** is a party with an interest in an enterprise; corporate stakeholders include investors, employees, customers, and suppliers.

Regulated industries, such as banking and healthcare will have requirements driven by the regulations governing their industries.

BUSINESS REQUIREMENTS

Recovery Point Objective (RPO)

is the age of data that must be recovered from backup storage for normal operations to resume if a system or network goes down

Recovery Time Objective (RTO)

is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

SLAs between a company and customers will influence RPO and RTO

BUSINESS REQUIREMENTS

Recovery Service Level (RSL)

measures the compute resources needed to keep production environments running during a disaster.

is a percentage measure (0-100%) of how much computing power you will need during a disaster

based upon a percentage of computing used by production environments versus others, such as development, test, and QA

Answers 'what needs to be migrated to keep production running?'

EXAMPLE: a 10-web server environment that uses 8 for dev, test, and QA, only 2 would need to be migrated for production.

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

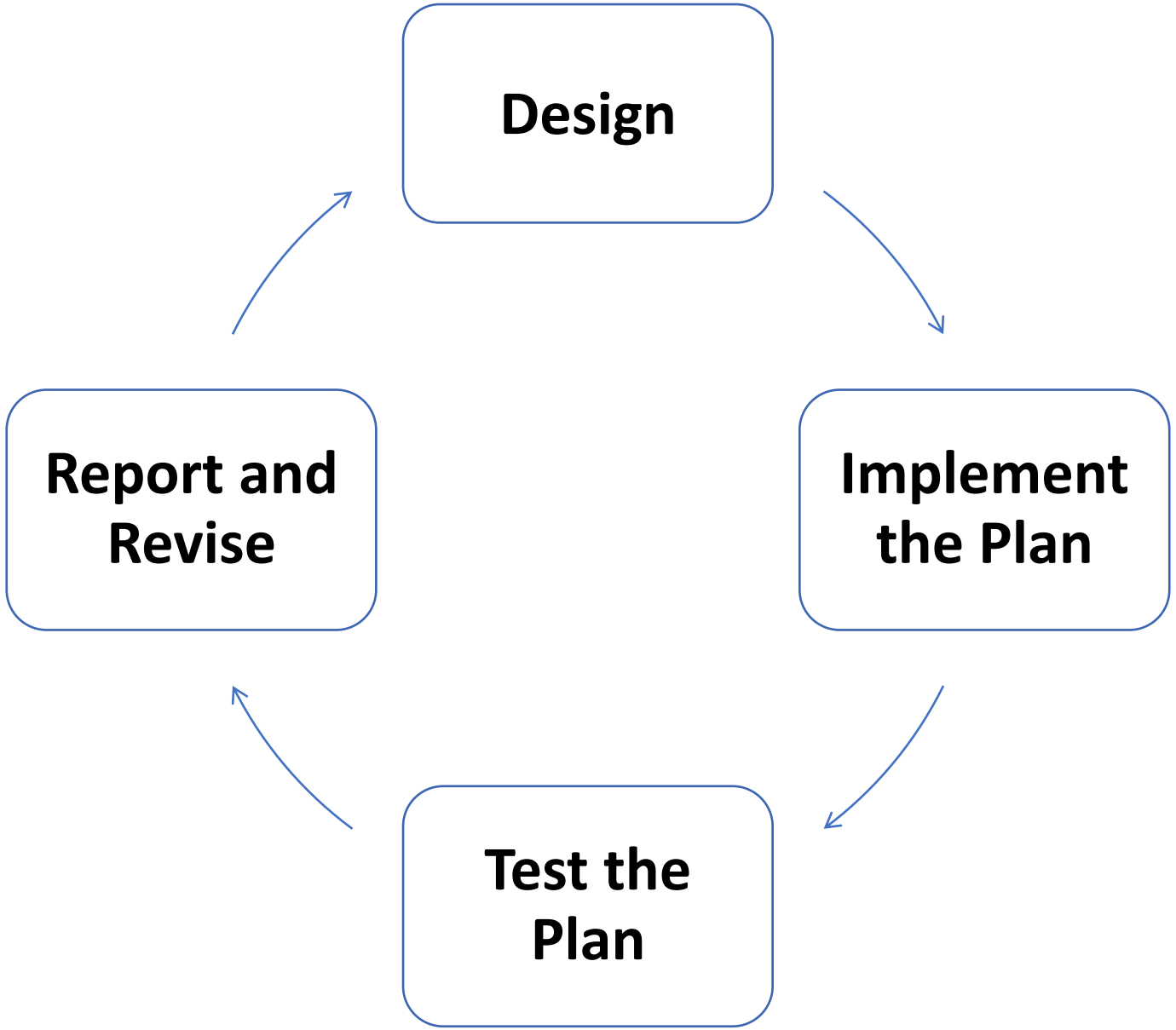
DEMO

Data backup and retention features in PaaS services

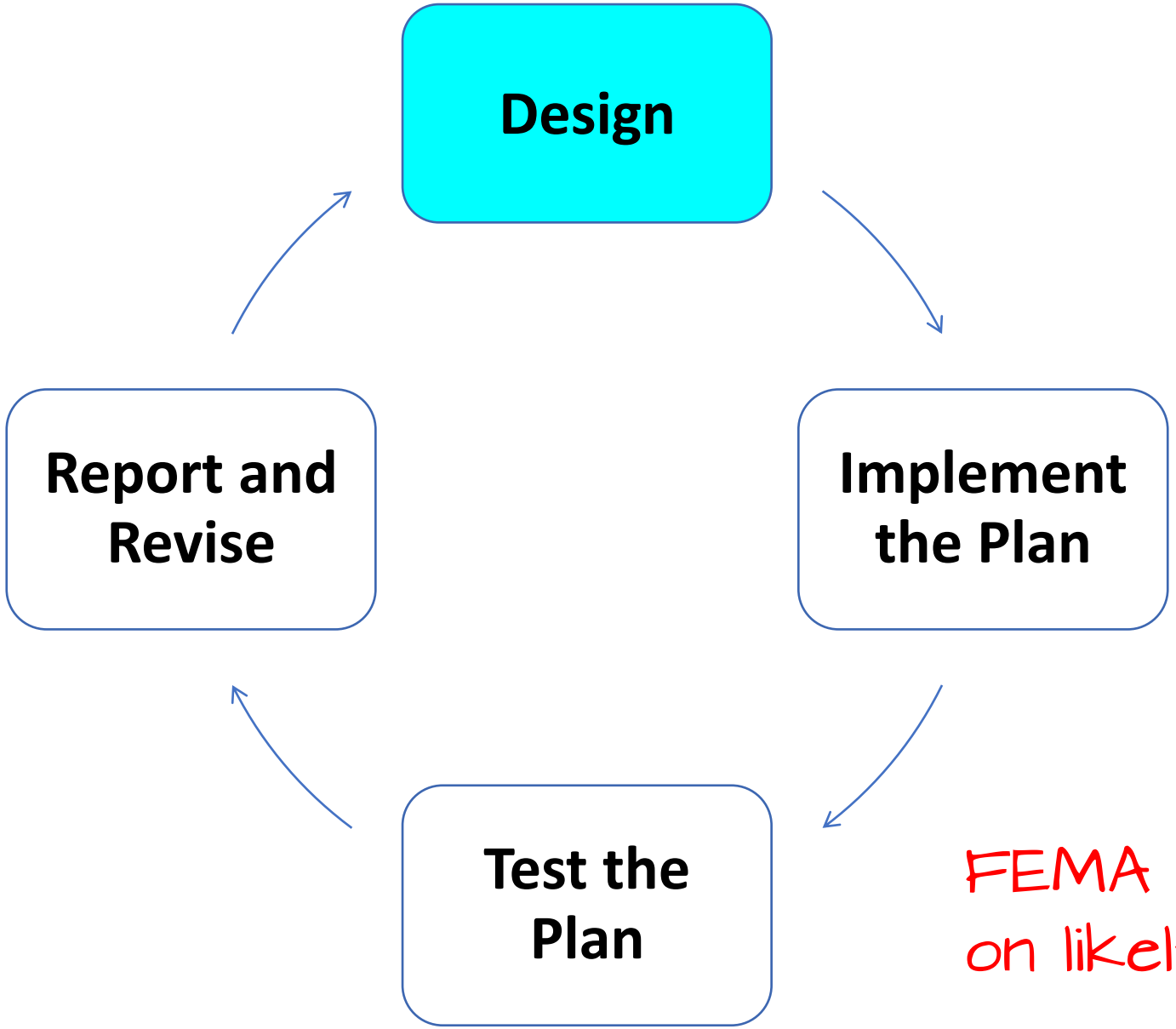
EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

INSIDE CLOUD AND SECURITY

BCDR PLAN CREATION, IMPLEMENTATION AND TESTING



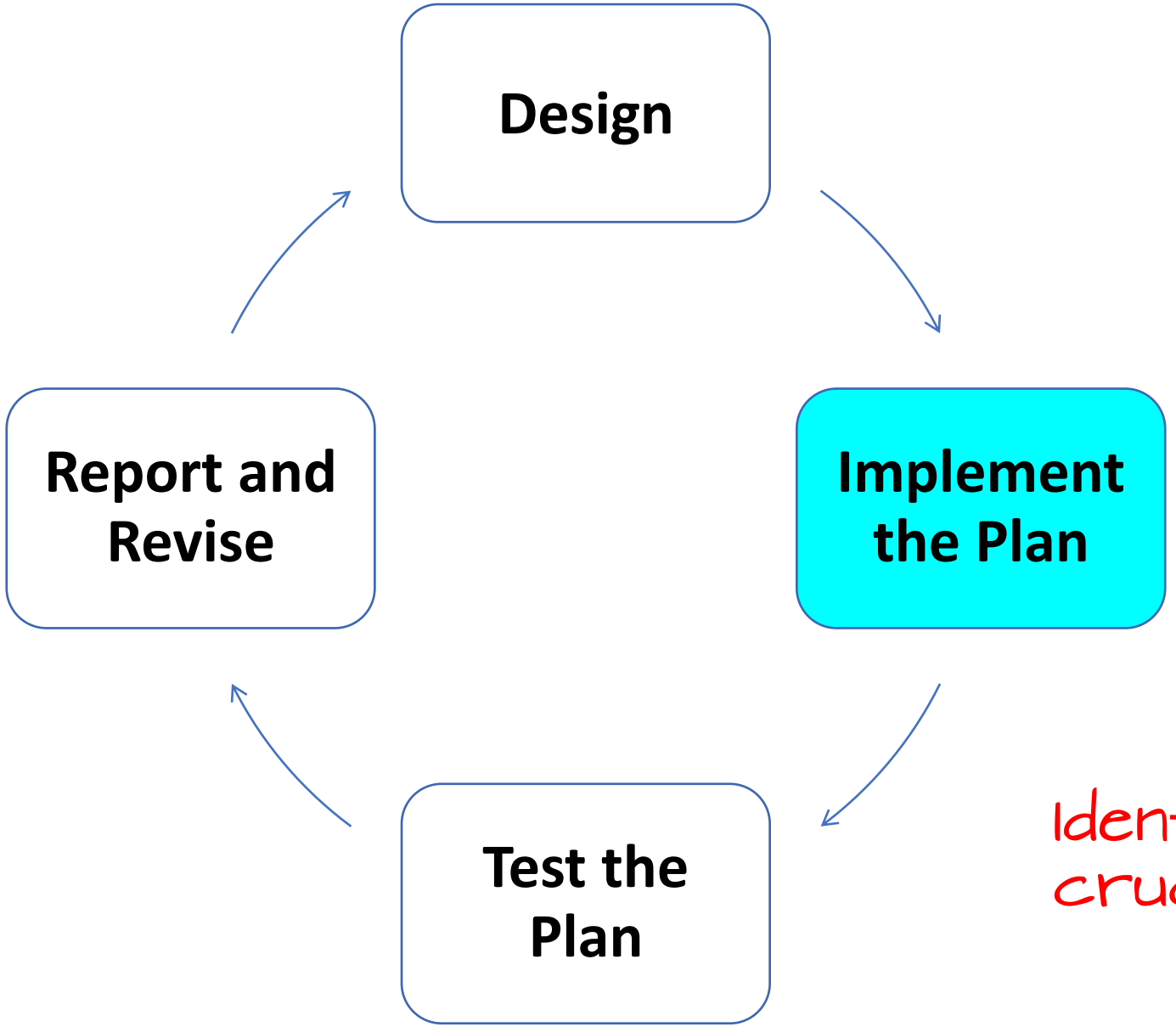
BCDR PLAN CREATION, IMPLEMENTATION AND TESTING



Based on priorities from the business impact analysis (BIA)

FEMA and Infragard can advise on likely disasters for a region

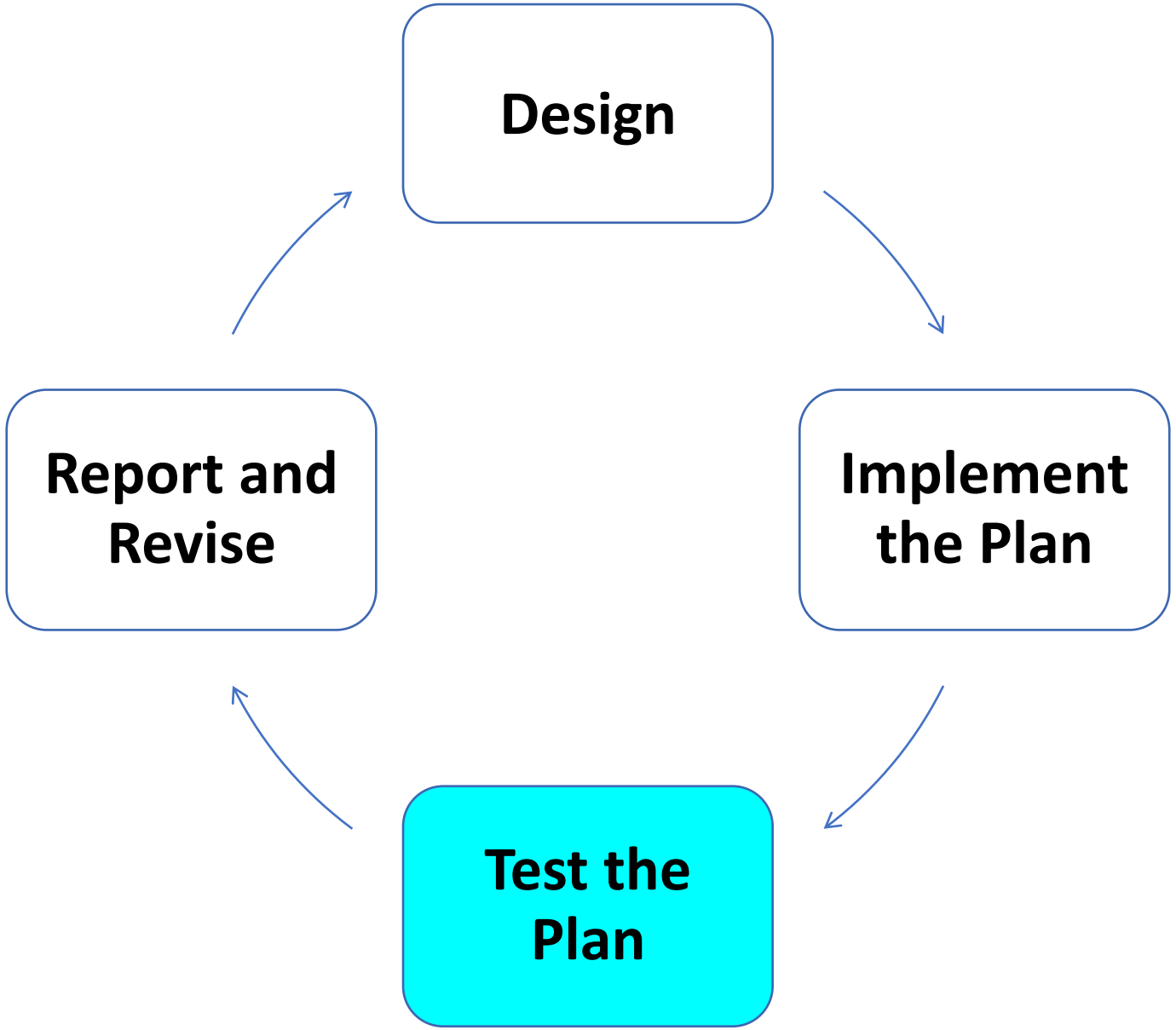
BCDR PLAN CREATION, IMPLEMENTATION AND TESTING



Implement the plan to protect critical business functions

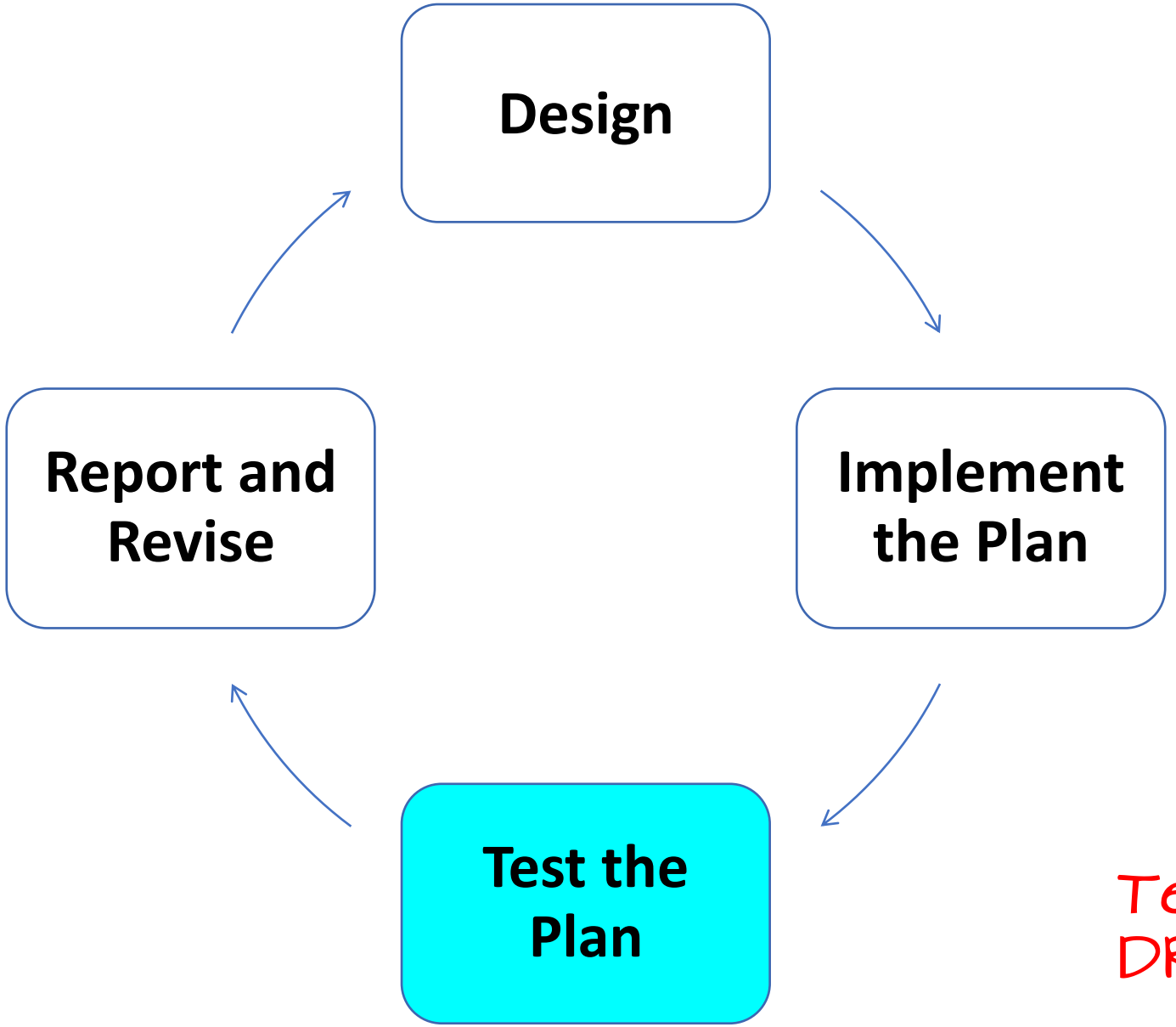
Identifying key personnel is a crucial implementation step

BCDR PLAN CREATION, IMPLEMENTATION AND TESTING



Testing ensures both the BCP/DRP function as expected

BCDR PLAN CREATION, IMPLEMENTATION AND TESTING

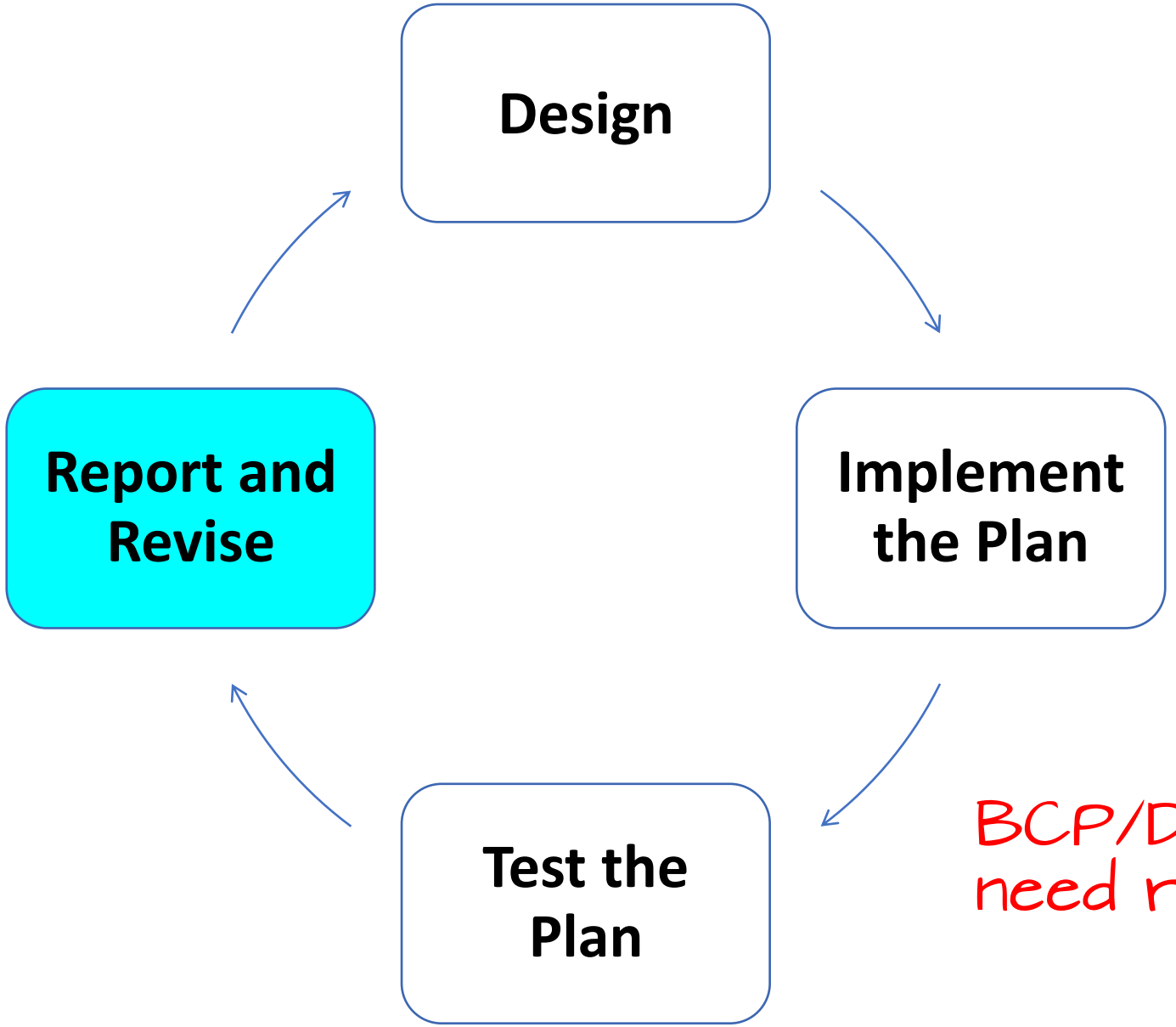


Testing ensures both the BCP/DRP function as expected

AND that people know their roles and responsibilities

Testing both BCP and DRP plans is essential

BCDR PLAN CREATION, IMPLEMENTATION AND TESTING



BCP/DRP should be revised as necessary based on test results

BCP/DRP plans evolve and need refinement over time

DRP TEST SCENARIOS

A BCP and DRP should be tested **at least annually**.

Common disaster scenarios include the following:

- ✓ Data breach
- ✓ Data loss
- ✓ Power outage or loss of other utilities
- ✓ Network failure
- ✓ Natural disasters *(e.g., fire, flooding, tornado, hurricane, or earthquake)*
- ✓ Civil unrest or terrorism
- ✓ Pandemics

The plan should test the most likely scenarios first and can be tested in a number of ways.

DISASTER RECOVERY TESTS

Tabletop testing

Members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.

Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting.

The team members refer to the document and discuss the appropriate responses to that particular type of disaster.

Role play only, minimal impact on productivity

DISASTER RECOVERY TESTS

Dry run

In this test, some of the response measures are tested (on non-critical functions).

Full test

Involves actually shutting down operations at the primary site and shifting them to the recovery site.

When the entire organization takes part in an unscheduled, unannounced practice scenario, of full BC/DR activities.

IMPLEMENTATION

The cost of building resiliency should be less than the cost of business interruption.

Implementing BCP or DRP processes may necessitate utilizing cloud computing for critical services.

Customers can take advantage of the cloud's high availability features like:

- ✓ multiple availability zones
- ✓ automatic failover to backup region(s)
- ✓ direct connection to a CSP.

These choices come with costs that must be considered.

The cost of high availability in the cloud is generally less than a company trying to achieve high availability on their own

THANKS

FOR WATCHING!