CIRRUS

8000 Ft. view of CCSP exam

Author: Prashant Mohan

Table of Contents

CCSP Exam Weight

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%**

CCSP Exam mindset

- CapEx to OpEx is the driving factor for cloud.
- Cloud customer is ultimately accountable for its security.
- Ensure all the roles and responsibilities are appropriately captured in the contractual agreement.
- Customer should own key management.
- Encryption or crypto shredding is the method for data deletion in cloud.
- Service Level Agreement is an important constraint in the cloud.
- Data held in the cloud need to be considered about different jurisdictions as data might be dispersed in multiple locations.
- Security in cloud doesn't come free.
- Cloud should be as secure as traditional Datacenters.

Preparing for Exam day

- Refrain from studying too much 24 hours before exam day. It is good to have a clean head to focus more on the day of the exam.

- Sleep early the day before the exam, and it's advised to take at least 8 hours of good sleep. The exam needs you to be alert and focused.

- On the day of the exam, have a good breakfast and reach your exam center at least 30 mins before the scheduled time. Please make sure you're carrying all the necessary documents before leaving for the exam center.

- Do read the NDA and agree within 5 minutes, as failing to do so will forfeit your exam without a refund or appeal.

- Read the question, re-read the question, and then read the given options. Please make sure you are totally convinced before submitting the response. The best way to prepare for this mindset is to do as many practice questions as possible. Understand why the choice is correct and why the other options are incorrect.

- Take breaks. It can't be emphasized enough the significance of taking breaks during the exam. Make sure you re-channelize yourself and then come back.

- In the end, relax. Trust your preparation. If you've prepared well, it's all going to end well! :)

Wish you all the very best with your Certified Cloud Security Professional exam!

About the author –

Prashant is an adept professional in Information Security with more than a decade of experience. He is well versed in assessing security for versatile domains like financial institutes, healthcare industry and service providers. He has given several best practices to have the process improvement and helped the organizations mitigate their risk.

Prashant also indulges himself in speaking on several webinars, security forums and has been actively mentoring aspiring security professionals in obtaining right career path and security certifications.

He has also authored CISSP study guide "The Memory Palace - A Quick Refresher For Your CISSP Exam "

You can connect him on LinkedIn here.

Note from Author –

CIRRUS – 8000 ft. view of CCSP course, as the name suggests, gives you a very high level understanding of the entire Certified Cloud Security Professional course. This book has been written with a purpose to provide a synopsis of CCSP course as recommended by ISC2 inline with the exam outline. You will notice several exam tips (you will see highlighted in *red*) throughout the book, which has been included to keep them in mind while attempting any questions. At the end of each domain, you would find exam essentials that include topics that include topics you have to pay extra attention from the examination perspective.

I want to dedicate this book to all security professionals who tirelessly work towards making a *safe* and *secure* cyberworld. Your commitment and perseverance are truly remarkable. Few people have always inspired me, and many others like me to give it back to the community. Thank you for all the selfless contributions you have made and are continuing to do so: Prabh Nair, Luke Ahmed, Fadi Sodah, Thor Pederson, Ben Malisow, Adam Gordon, Wentz Wu.

Thank you Infosec Train for publishing this!

A special mention to Radha Arora, who has worked day and night with me to make this book a wonderful format. This book wouldn't have been possible without your continuous support.

Disclaimer

- This document is entirely free for anyone preparing for their CCSP exam. It is not meant for sale or as part of a course. It is purely a contribution to align with the Fourth Canon of the ISC2 Code of Ethics to "Advance and Protect the Profession."

- This book has been written to have all the CCSP concepts handy at one place. It is an original creation of the author. However, a few terms, concepts, tips, images, and language(s) result from inspiration and derived from multiple sources (books, videos, notes). The intent is not to violate any copyright law(s). If the reader comes across any text, paragraph(s), image(s) which are violating any copyright, please contact the author at prashantmohan.cissp@gmail.com so that this can be removed from the book.

- The content is entirely on the guidelines of ISC2, and I've tried my best effort to make them as simple as possible for others to understand. This document is not affiliated with or endorsed by ISC2.

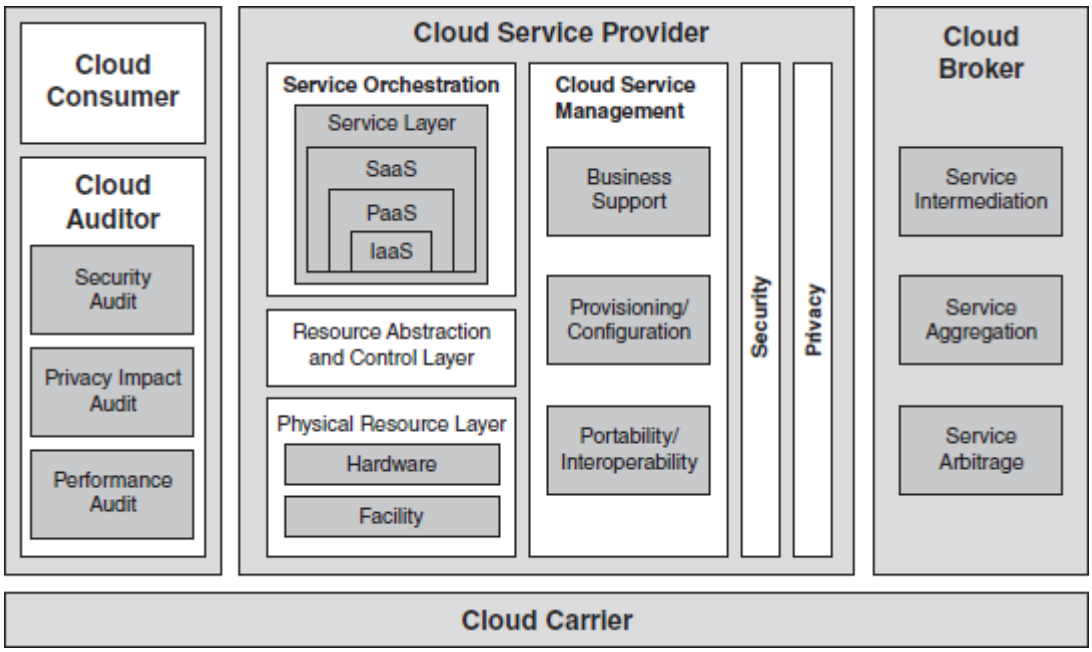
"CIRRUS - *Cirrus clouds are short, detached, hair-like clouds found at high altitudes. The CIRRUS is also an aircraft model which is a single-engine four- or five-seat composite aircraft."*

- Source Courtesy: Internet

Domain 1 – Cloud Concepts, Architecture and Design

Cloud Computing: It is a model for enabling ubiquitous, convenient, on-demand network access to a shared proof of configurable computing resources that can be rapidly provisioned and released with minimal management effort of service provider interaction.

--NIST Definition



Cloud Computing Overview

Managed Service Provider (MSP): **Customer dictates** the technology and operating procedure.

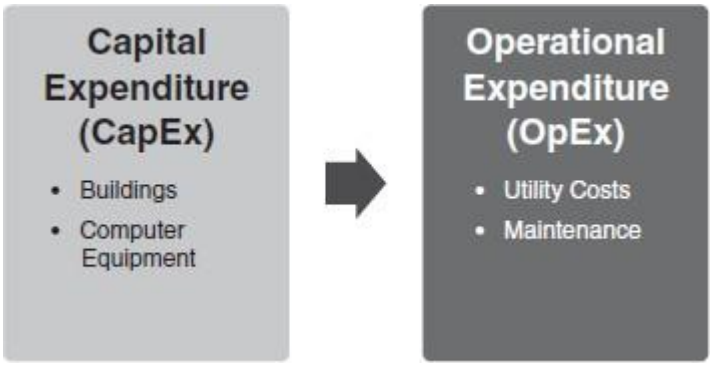
MSP has the following characteristics:

- Some form of NOC services.
- Some form of Helpdesk.
- Remote monitoring and management of all or most of the objects.
- Proactive maintenance under the management of customer.
- Delivery of these solutions.

Cloud Service Provider (CSP): **The Service Provider dictates** both technology and operational procedures being made available to cloud customers.

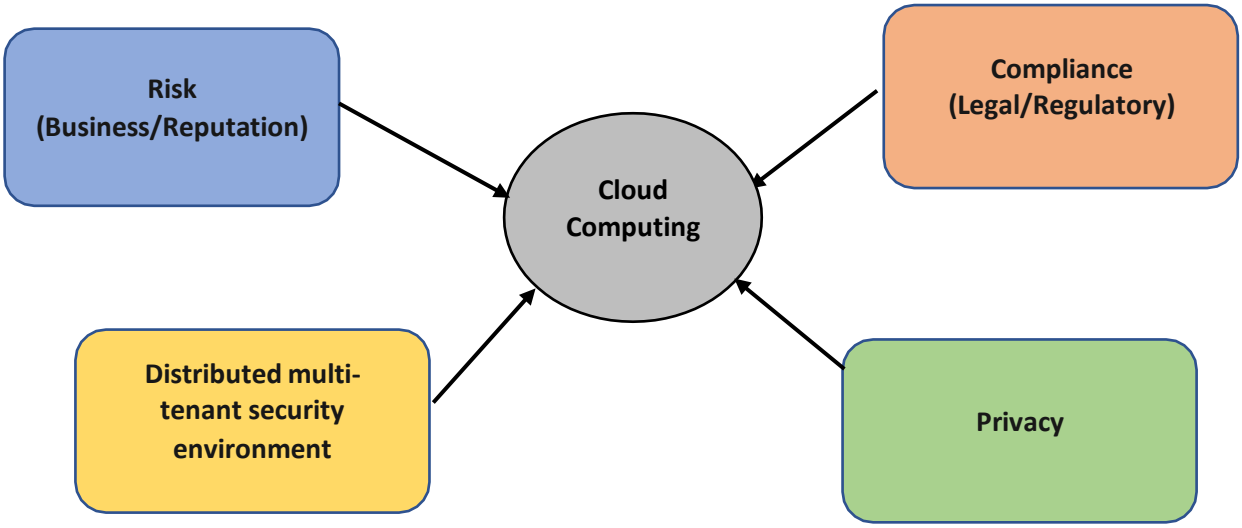
**Exam tip: It's good to know the difference between MSP and CSP.*

Drivers of Cloud computing



Drivers that move companies towards cloud computing

- **Reduce IT complexity**
  - Risk reduction
  - Scalability
  - Elasticity
- **Consumption-based pricing**
  - Virtualization
  - Cost (*pay per use*)
- **Business Agility**
  - Mobility (*access from anywhere*)
  - Collaboration and innovation



Cloud computing issues concerns

Reputational Risk: The loss of the value of a brand or an organization's ability to persuade.

Ways to manage reputational risk:

- Strategic alignment
  - Effective board oversight
  - Integration of risk into strategy setting and business planning
- Cultural alignment
  - Strong corporate values and focus on compliance
- Operational focus
  - Strong control environment

It would be incorrect to say that Cloud Computing is insecure than a traditional on-premise solution without comparing it side by side through several parameters.

**Exam tip: Extensive use of automation helps in providing continuous security monitoring and reporting.*

Cloud Computing Roles:

- **Cloud Backup Service Provider:** Third Party, which manages **cloud-based backup responsibility**.
- **Cloud Computing Reseller:** Company that purchases service from CSP and **sell it further to customers.**
- **Cloud Customer:** An individual or entity who **subscribe to cloud-based services**.
- **Cloud Service Auditor:** Third party, which verifies the attainment of SLA agreement.
- **Cloud Service Brokerage:** Third party which liaison between a customer and CSP. They are typically the resellers.
- **Cloud Service Provider (CSP):** Company that provides cloud-based platform, infrastructure, application to other organizations as a service.

Key Cloud Computing Characteristics:

****Thumb rule for choosing a CSP***

- **On demand self-service:** Although it comes with a risk as people can provision themselves without using approved transaction methods(credit card).
- **Broad Network Access:** Information should be available at any point from anywhere. Challenges are using mobile devices, as no security controls are present.
- **Resource Pooling:** Ensuring ideal resources are adequately distributed among the customers to have full utilization.
- **Rapid Elasticity:** Allow users to obtain additional resources, space, etc. as required to meet the workload. If this is done locally, CapEx is high.
- **Measured Service:** Pay as you use.

Exam tip: **RAM, CPU, Storage, and Networking are the building blocks of Cloud Computing.*

Note: IaaS has the most fundamental building blocks.

Cloud Computing Functions:

- **Cloud Administrator:** Responsible for implementing, monitoring, and maintenance within the organization or on behalf of a Third party. Works directly with system, network, and cloud storage admin.
- **Cloud Application Architect:** Responsible for porting, adapting, and deploying the application to the cloud. Works with development and other integration teams to ensure the application is reliable, secure throughout the lifecycle.
- **Cloud Architect:** Determines when and how private cloud meets the policies and contractual requirements from a technical perspective.
- **Cloud Data Architect:** Similar to cloud architect. Manages the various storage types and mechanisms utilized within cloud environment. Takes care of SLA.
- **Cloud Developer:** Focus on the development of cloud infrastructure.
- **Cloud Operator:** Maintains day to day operation tasks from maintenance to monitoring.
- **Cloud Service Manager:** Responsible for policy design, business agreement, pricing model and some elements of SLA (Contractual amendments). Works closely with could management and customer.
- **Cloud Storage Administrator:** Focus on mapping, segregation, bandwidth, and reliability of volume storage. It ensures SLA is met.

Cloud Services

- **Infrastructure as a Service (IaaS):** Consumers can provision (subscribe) processing, storage, network, and other fundamental computing resources and deploy their own Softwares and OS.

Consumer	**CSP**
OS	Storage
Software	Network
Host Firewall	Processing

Key Components and Characteristics:

1. **Scale**: Should be able to support significant workloads.
2. **Converged network and IT capacity pool**: Virtualization and service management component across network with appropriate services. From a user perspective, the pool appears seamless and endless for both servers and network. They always support SLA.

3. **Self-service and on-demand capacity**: Portal where customers can look into the resource utilization and add, remove, manage resources without interacting with CSP.

High reliability and resilience: Should be reliable and resilient while enforcing and meeting SLA.Benefits:

1. Metered usage and price basis on the units consumed.
2. Ability to scale up and down based on actual usage.
3. Reduced cost of ownership, maintenance, and support.
4. Reduced energy and cooling cost.

- **Platform as a Service (PaaS):** Also known as Cloud OS. Capability provided to customers to deploy application using programming language, libraries, services, and tools supported by providers.

Consumer	**CSP**
Application	Infrastructure
Configuration	Network, storage
Data	OS

Key Components and Characteristics:

1. **Support multiple language and frameworks:** Customer can leverage the platform in developing application based on their requirement and choice.
2. **Multiple hosting environments**: Should migrate from public, private cloud to hypervisor or bare metal. This can also be used as a form of contingency.
3. **Flexibility**: Any plugin can be introduced to the platform.
4. **Allow choice and reduce lock-in**: Customers should have options with no restriction.
5. **Ability to auto-scale**: Use as per the requirement. Resource allocation is done as per the requirement.

**Lock-in: Also known as vendor lock-in, customers are bound to stay with a service provider due to situations like using proprietary format or unfavorable contractual agreements.*

Benefits:

1. Operating system can be changed and updated frequently.
2. Distributed teams can work on the same project.
3. Services are available and can be obtained from diverse sources.

4. Single vendor reduces cost.

Software as a Service (SaaS): Customer access the application provided by CSP, which is running on cloud infrastructure. e.g., YouTube, Office 365.

Consumer	CSP
Data	Infrastructure
	Network, storage
	OS, Servers, Application

SaaS Delivery Model:

- **Hosted Application Management (HAM)**: Hosts software for customer and makes it available over the internet.
- **Software on demand**: Pay as you go. The application is hosted on shared infrastructure (O365, Gmail etc.).

Benefits:

1. Overall reduction of cost: One of the major benefits of adopting a cloud environment eradicates buying hardware and supporting infrastructure.
2. Application and software licensing: CapEx is removed and replaced by pay per use model.
3. Reduced support costs: CSP handles the support, and it's a part of the agreement:
    a. Ease of use and limited administration
    b. Automatic updates and patch management
    c. Global accessibility

Cloud Deployment Models

Identifying which cloud model should be adopted, should be influenced by the organization's risk, appetite, cost, compliance, regulatory requirements, and legal obligations.

- **Public Cloud:** It can be used by anyone and have multiple tenants from various businesses. It exists on the premises of CSP.

Benefits

1. Easy and inexpensive
2. Streamlined and easy to provision resources
3. Scalability to meet customer needs
4. No wasted resources

- **Private Cloud:** Cloud infrastructure exclusively for a single organization. May be owned and managed by the organization or Third party. Exist on or off-premise a.k.a organisation's internal cloud.

Benefits

1. Increased control over data, applications and systems
2. Ownership and retention of governance controls
3. Assurance over data location and removal of multiple jurisdiction, legal and compliance requirement

- **Hybrid Cloud:** Two or more distinct cloud infrastructure (Public, Private or Community). Retain control of IT environments.

Hybrid = Public + Private

(Non-mission critical) (Mission critical)

Saves cost Security

Benefits

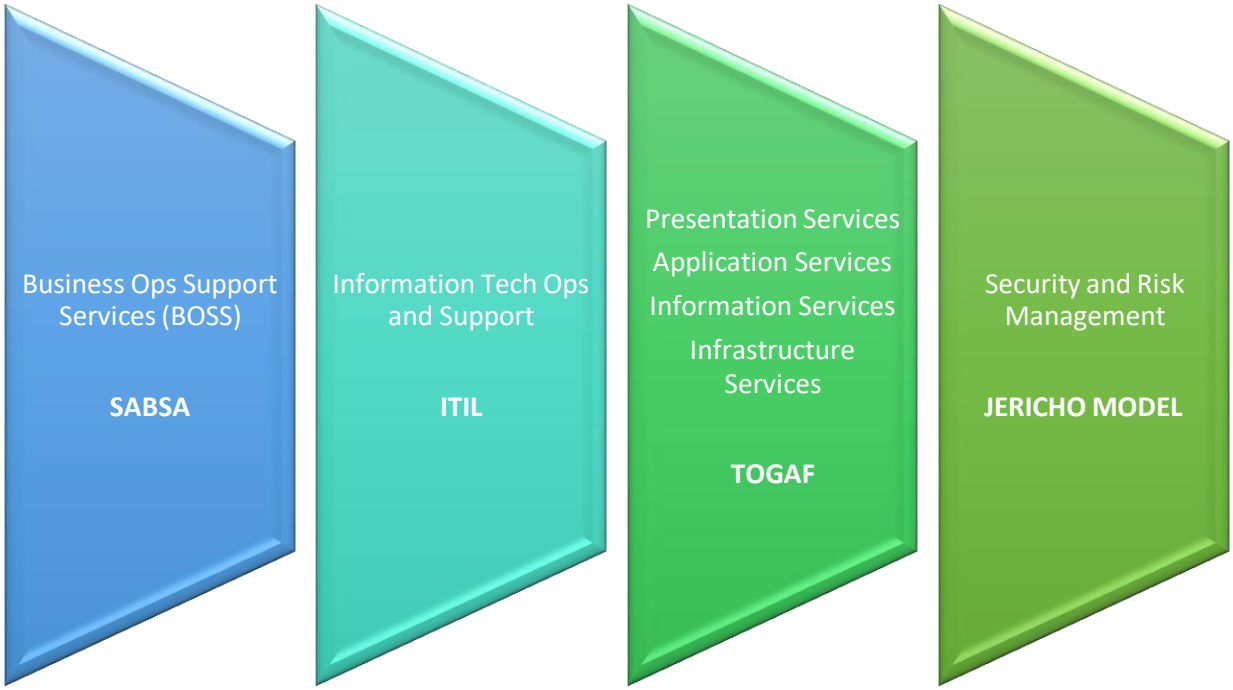
1. Retain ownership and oversight of critical tasks
2. Reuse previous investment in technology within the organization
3. Control the most critical business component and system
4. Cost-effective way of fulfilling a non-critical business function
5. Enhance *cloud bursting* and Disaster Recovery

**Cloud Bursting: When private cloud workload has reached a maximum limit, public cloud resources are being used.*

- **Community Cloud:** Used by customers with similar business objectives. e.g., all customers belonging to health care would choose a similar SaaS solution. Exists on or off-premise.

**Exam tip: Choosing Cloud solution should be a business decision.*

Architecture Overview



CSA Enterprise Architecture

NIST Cloud Technology Roadmap

- **Interoperability:** It defines how easy it is to move or reuse application components regardless of provider, platform, OS; application component work together etc.
- **Portability:** Key aspect in selecting CSP as it can help in preventing vendor lock-in.
- **Availability:** Systems and resources availability defines the success and failure of CSP. There should not be a single point of failure (SPOF) and should have at least 99.9% availability.
- **Security:** Should be a part of a contractual agreement stating minimum security requirement. CSP also have a NDA signed. (MORE SECURITY = MORE COST)
- **Privacy:** It's a significant challenge for CSP and customers as there's no uniform privacy law. Should be a part of the contract and SLA. EU countries have it included in EU Data Protection Law (Now GDPR).
- **Resiliency:** Cloud infrastructure continues to operate in the event of disruption or disaster.
- **Performance:** Cloud computing and performance should go hand in hand. Should focus on **Network, Compute, Storage,** and **Data** (Design, integration and development activities)
- **Governance:** Process and decision to define and assign responsibilities and verify performance. Extension of traditional governance.

- **SLA:** If CSP fails to provide services in the decided time, the financial stipulation should be invoked.

- **Auditability:** Access to report and obtain evidence. It gives customer the confidence while choosing CSP.

- **Regulatory Compliance:** Organization's requirement to adhere to relevant regulations (e.g. PCI-DSS, HIPAA etc.).

Impact of related technologies

Cloud computing provides the foundational IT services for most business related capabilities including:

- Machine Learning
- Artificial Intelligence
- Blockchain
- Internet of Things (IoT)

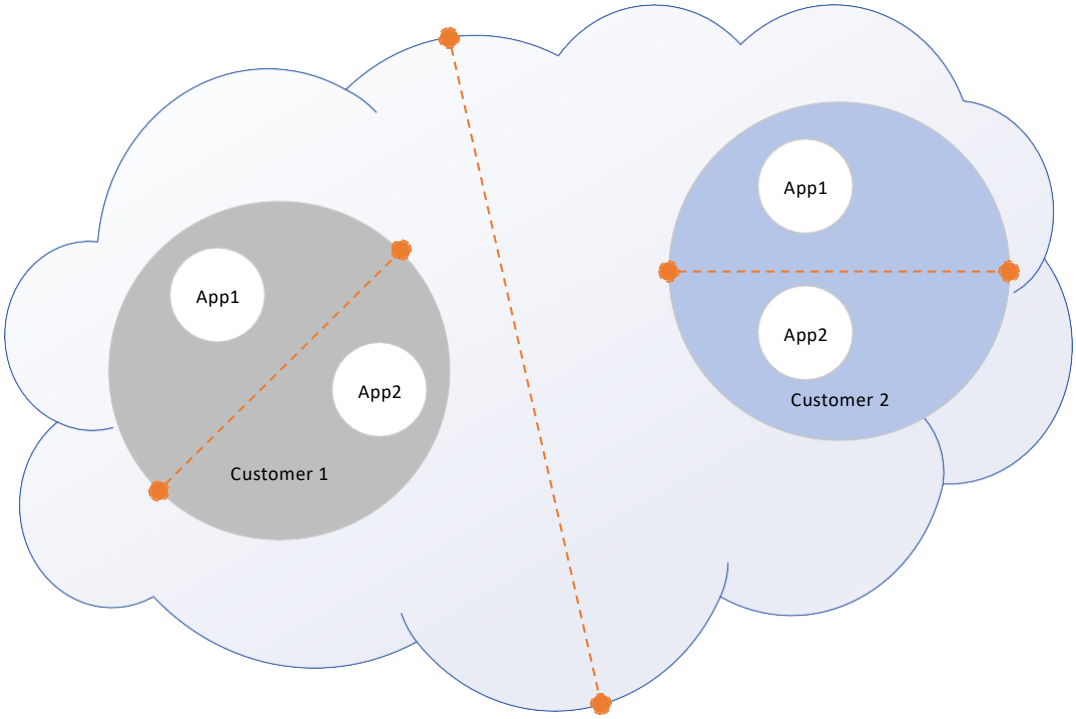
These technologies are made easily and economically available to the customers by the automation, elasticity, and resource pooling capabilities of cloud computing. Apart from this, if used properly, these technologies provides a lot of ease for enhancing their business models with great security.

Network Security Perimeter

- **Physical Security:** It ensures access to the cloud service is adequately distributed, monitored, and protected by underlying physical resources when the service is built-in..

- **Logical Security:** It consists of link, protocol, and application layer services.

For many cloud networks, the perimeter is the demarcation point. For other cloud networks, the perimeter is dynamic micro-borders around individual customer solutions or services.



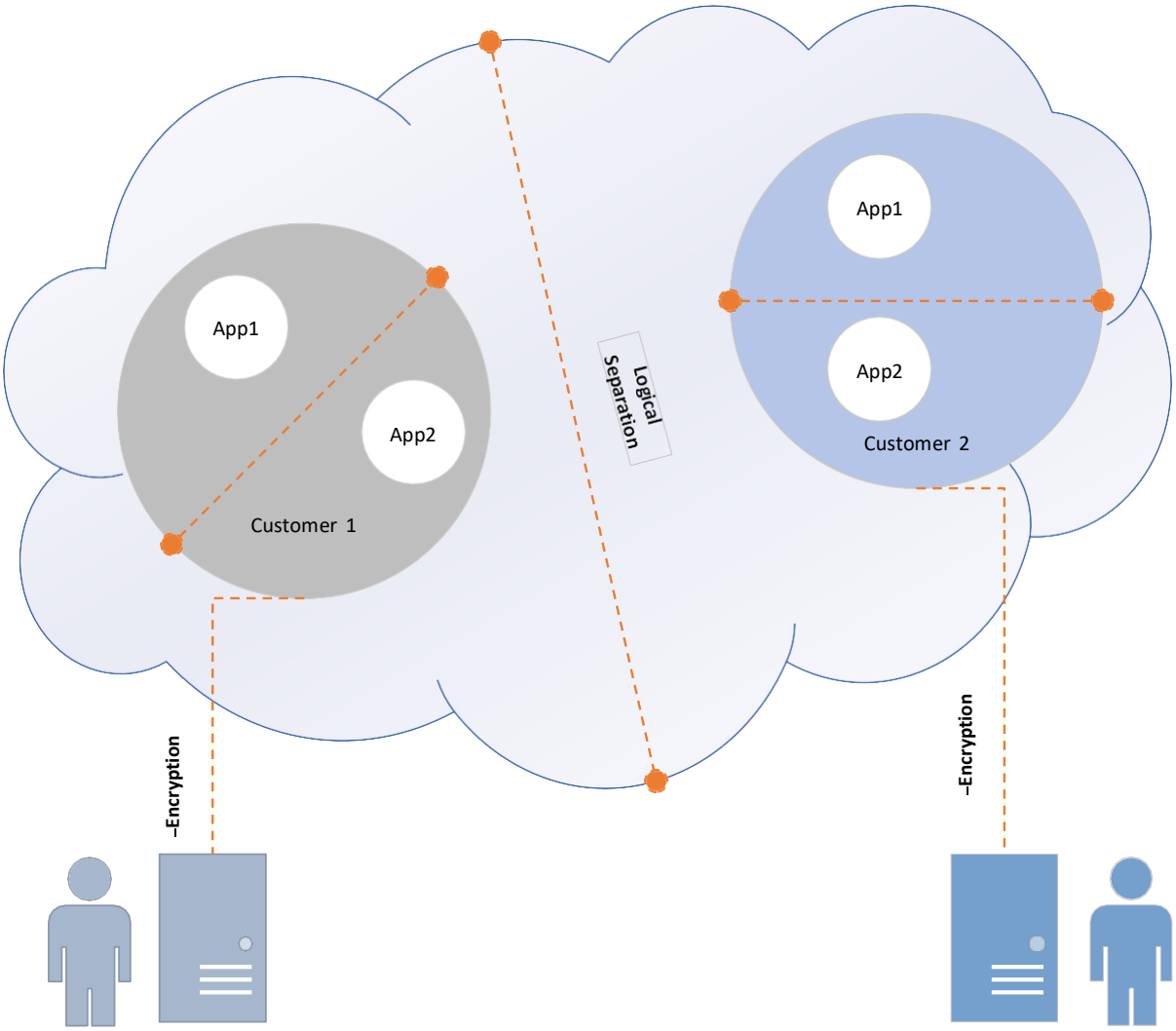
Micro-boundaries separating customers and services

In other cloud networks, there may be no perimeter at all. (No Segregation)

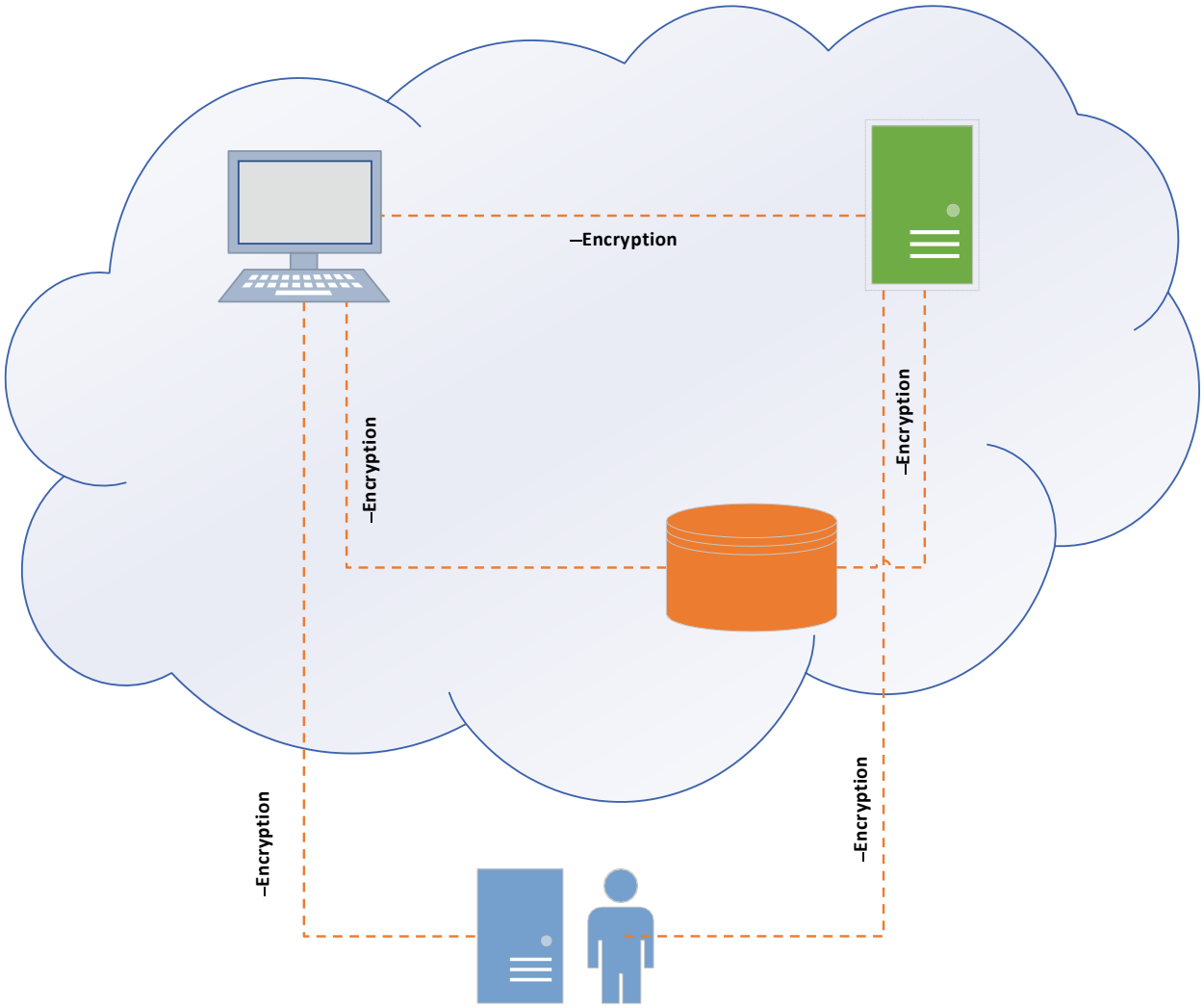
Cryptography: Required for the protection of sensitive information (confidentiality). It is majorly dependent on:

- Strong Key Management
- Secure Key Management

Encryption Critical Success Factor (CSF): Enable secure and legitimate access and enforcing control against unauthorized access.



Separation of tenants in Public Cloud



Encryption in Private/Hybrid Cloud

- Data in Motion (DIM): All the connections from host to cloud should be encrypted in transit (TLS 1.2).
- Data at Rest (DAR): Data is stored in the database, or any repository should be encrypted (AES 256).

**Exam tip: If the data is encrypted at CSP, in case of any dispute, it will be challenging to extract your own data if CSP owns key management process. Apart from this, encryption also affects performance.*

Key Management

Single person should never handle encryption. Encryption and Separation of Duties (SoD) should always go hand in hand. Key management should be separated from CSP.

Data owner should be responsible for:

- Encryption
- Control and manage the key management process
- The storage location of encryption keys (preferably On-premise)

Common approaches of key management:

1. Remote key management service: Customers maintain KMS on the premise. Connectivity is required between CSP and customers for encryption and decryption.

2. Client-side key management system: Similar to KMS. CSP provide KMS to customer and KMS resides on the customer's premise. For SaaS, this is the best solution.

Key Management Options

- XML Key Management Specification: This specification defines protocols for distributing and registering public keys, suitable for use in conjunction with XML Digital Signatures and XML Encryption.

- Key Management Interoperability Protocol: It defines message formats for manipulating cryptographic keys on a key management server. KMIP also explains messages that can be used to perform a cryptographic operation on a server such as encrypt and decrypt.

- Trusted Platform Module: Cloud-based software applications can use a Trusted Platform Module (TPM) to authenticate hardware devices. A TPM is a chip placed on the main board of the device, such as a laptop. It may also be used to create and store keys as well as perform tasks as a cryptoprocessor.

- Hardware Security Module: A hardware security module (HSM) is a physical computing device that provides crypto processing and safeguards and manages digital keys for strong authentication.

Identity and Access Management

Key Phases:

1. Provisioning and Deprovisioning:
   Identification ➔ Authentication ➔ Authorization ➔ Auditing ➔ Accountability

2. Centralized directory service: It is a foundation of IAM and security. X.500, LDAP, Privileged Identity Management (PIM), etc. It stores, processes and facilitates a structured repository of information stored coupled with unique identifiers and locations.

3. Privileged User Management: Should track the usage (auditing), authentication success and failures, authorization dates, and time enforce password management. Separation of Duties should be implemented to reduce risks.

4. Authorization and Access Management: These are point in time activities that rely on the accuracy and on-going availability of resources and functioning process, SoD, Privileged User Management, Password Management etc. If one activity is not carried out regularly, it weakens entire security posture.

**Exam tip: Minimum 2 Factor Authentication should be preferred.*

Data and Media Sanitization

If you want to switch CSP, make sure all the data is adequately sanitized and make it inaccessible.

1. Vendor lock-in: When customer cannot migrate to other CSP due to technical or non-technical constraints. If records are high, open API mechanism can reduce this challenge.

**Exam tip: Vendor lock in can happen due to using proprietary data or unfavorable contractual agreements. As a customer, it should be strongly considered on how to avoid vendor lock-in*

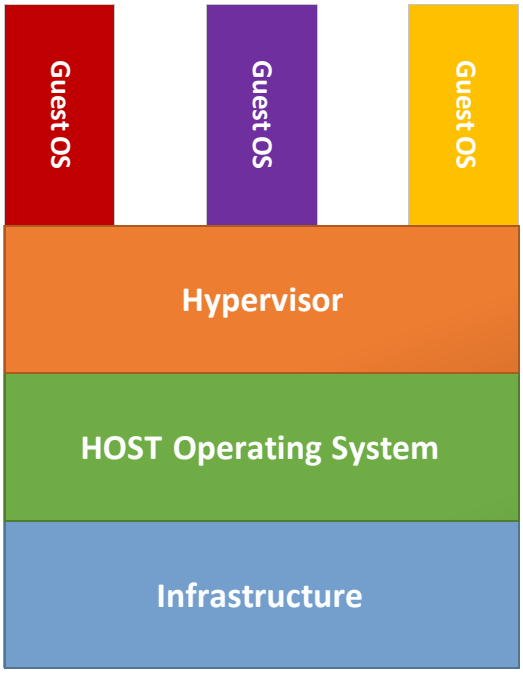
2. Cryptographic Erasure: This is the most common technique to delete the data stored in cloud. The process is to encrypt the data and destroy the keys so that it's not recoverable. This process will be challenging if the key management process is handled by CSP.

3. Data Overwriting: Overwriting data multiple times. It's not suitable for highly classified data e.g. PII etc.

Virtualization Security

Virtualization is a key target for attackers. The hypervisor can be the most vulnerable component.

Hypervisor: It controls the host processor and resources, prioritizing and allocating what is needed for each OS.



Virtualization

Type 1 Hypervisor (Hardware): Running directly on hardware with VMs resources provided by the hypervisor. eg. Citrix. It has a reduced attack surface than Type 2 Hypervisor because the vendor controls relevant software.

Type 2 Hypervisor (Operating System): Runs on Host OS. As it's OS based, it is more prone to attack as OS has a lot of vulnerabilities. Lack of standardization on OS opens up additional exposure.

Common Threats

Data Breaches: Cloud computing has widened the scope of data breaches as BYOD comes in picture (mobile devices) and expects more breaches. Any data breach (HIPAA, PII, PCI-DSS) needs to be reported to relevant bodies.

Data Loss: Loss of information due to deletion, overwriting, corruption or integrity-related issues.

- Who owns the responsibility of data back up?
- Once the data is corrupted, can it be restored?
- Restoration happens on a shared platform.

If encrypted data is uploaded, encryption keys need to be protected. If the keys are lost, data will not be accessible.

Account or service traffic hijacking: Phishing, Smishing etc. is used to highjack a service and then steal credentials (session hijacking).

Insecure interfaces and APIs: Cloud resources are accessible by the APIs provided by CSP.

Denial of Service: Should avoid a single point of failure.

Malicious insiders: To secure any organization's key asset, we need **P**eople, **P**rocess, and **T**echnology.

Abuse of cloud services: Attackers can also host malicious Softwares on cloud. Proper segmentation should be there.

Insufficient Due-Diligence: What if the CSP goes bankrupt, can we change the CSP? If CSP fails, ensure financial stipulation is included in the contract.

Shared technology vulnerabilities: CSP shares infrastructure and technology not only with tenants but also with other CSPs. Layered protection/defense in depth is important.

Security Consideration for Different Cloud Categories

IaaS Security

- **VM attacks:** VMs on the same physical machine can attach each other because they share same Hardware and Software resources (Hypervisor).

- **Virtual Network:** It contains virtual switch software that controls the traffic between virtual NIC and physical NIC.

- **Hypervisor attacks:** Compromising hypervisor will give control over VMs. Common attacks are:
    - Hyper-jacking: Installing rogue hypervisor that can take complete control.
    - VM escape: Crashing the guest OS to get out of it and running an arbitrary code in the host OS. This allows malicious VM to take control over the host OS.

- **VM Based Rootkits**: Installing malicious hypervisor on the fly or manipulation to gain control.

- **Virtual Switch attacks:** Modification of switch configuration, VLAN, and trusted zone and ARP tables.

- **DoS Attacks:** Misconfiguration at the hypervisor can make one VM to utilize all the resources making other VMs unavailable.

- **Colocation:** Multiple VMs residing on a single server and sharing the same resources increases the attack surface and risk of VM to VM and VM to Hypervisor compromise.
    - Physical server is offline ➔ safe from attack
    - VM is offline ➔ can still be attacked, malware infections due to the unavailability of patching

- **Multitenancy:** Information leakage, VM to VM and VM to Hypervisor compromise.

- **Loss of control:** Users don't have control over the location of the data centers and services, and CSP is not aware of the content which they run.

- **Network topology:** Due to a lot of changes in cloud (VMs are being added or removed or moved from one host to another) creates a challenge for network topologies.

- **Logical network segmentation:** Isolation is important for sensitive information. VLAN, NAT, Bridging etc.

- **No physical endpoints:** Due to virtualization, physical endpoints (switches, servers, NIC) have been reduced.

- **Single Point of Access:** Hosts have limited NIC to all VMs.

PaaS Security

- **System and resource isolation:** Should not have shell/root access of the servers running. Admin should be segmented.

- **User-level permission:** Each instance should have its own permission. We need to ensure no authorization creep is there (accumulating privileges over the time).

- **User access management:** Helps to protect CIA of an asset. Key components are:

    - **Intelligence:** Collection, analysis, auditing, and reporting based on organization policies.
    - **Administration:** On-boarding/off-boarding or changing account access on system.
    - **Authentication:** Multi-factor authentication should be enabled.
    - **Authorization:** Least privilege should always be applied.

- **Protection against malware, backdoors, and trojans:** Once the backdoor is created, it creates a permanent attack surface.

SaaS Security

- **Data Segregation:** Customer's data can be stored in the same location with multiple tenants. Proper segregation should be implemented not only at the physical level but also at application level.

- **Data Access and policies:** Access to customer's data should be reviewed, logged, and monitored. CSP policy should match the customer's policy.

- **Web Application Security:** Given a large number of co-located tenants, if a vulnerability is exploited, CSP and customer will have a catastrophic situation.

Cloud Secure Data Lifecycle

Data is the single most valuable asset for an organization. The value of asset decides the security control.

- Create: Data is created.
- Store: Data is committed and stored in the repository.
- Use: Data is used (not including modification).
- Share: Information is shared.
- Archive: Data leaves active use and enter long term use.
- Destroyed: Data is permanently destroyed.

It's important to know the logical and physical location of the data to satisfy the audit. It's also important to know who is accessing the data and how they are accessing it.

Information and Data Governance Types

- Information classification
- Information Management policies
- Location and Jurisdictional policies
- Authorization
- Custodianship

Business Continuity Planning and Disaster Recovery

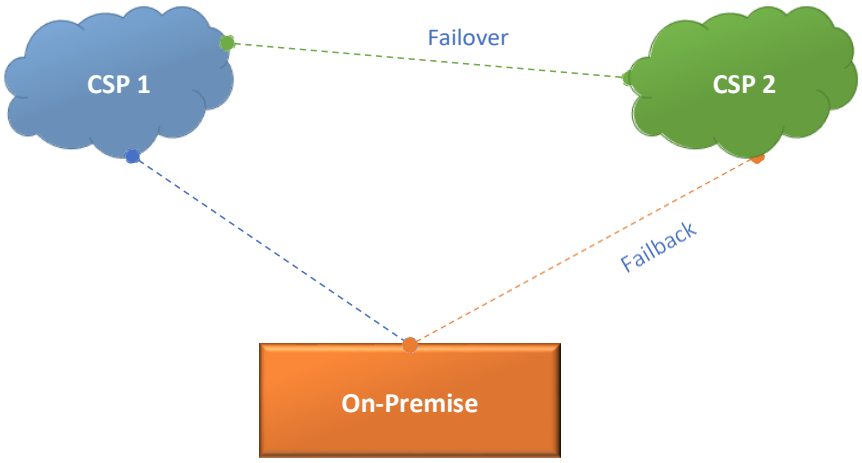
- **Business Continuity Element:** Many security professionals struggle to keep their BCP current as they have started utilizing cloud-based services. Not all assets are equal. What are the key fundamental components required to ensure business or service running?

- **Critical Success Factor:**

    - Understand your responsibility vs. the CSP responsibility:
        - Interdependency
        - Priority of restoration

        - Need for backup with other CSP
    - The agreement should have SLA which clearly addresses BCP/DR:
        - Penalty
        - RTO and RPO
        - Loss of integrity
        - Point of contact and escalation process

- **Important SLA Components:**
    - Undocumented Single Point of Failure should not exist
    - Migration to alternate CSP should be possible
    - Where data backups are included, incremental back-ups should allow the user to select the desired settings (coverage, frequency).



Choosing Alternate CSP as a BCP/DR plan

Cost Benefit Analysis (Cost Vs Risk):

- Resource Pooling: This characteristic makes cloud environment a lot economical option.
- Shift from CapEx to OpEx: Focus on core business and outsource non-essential IT operations.
- Factor in time and efficiencies: A lot of time is saved if cloud is chosen.
- Include Depreciation: Just like cars, technology also has depreciation, opt for cloud to avoid cost on depreciation.
- Reduction in maintenance and configuration time.
- Utilities cost: Choosing cloud can reduce costs significantly.
- Software and licensing costs.
- Pay per usage

Certification Against Criteria

"If it cannot be measured, it can't be managed."

There are no international cloud security standards.

ISO27001 – Standard

ISO27002 – Framework

ISO 27002:2013 – Provide guidelines

ISO27017:2015 – Guidelines for information and use of cloud services by providing additional implementation guidance for relevant control specified in ISO/IEC 27002. Provides control and implementation guidance for both CSP and Customer.

**Exam tip: it's essential to know above mentioned ISO standards*

System and Organization Control: Statement of Auditing Standard 70 (SAS70) was replaced by Service Organization Control (SOC) Type 1 and Type 2 reports.

Type 1: Point in time and test Design Controls

Type 2: 6 months to 1 year and test effectiveness of those controls

SOC 1 – Accuracy and completeness of product/service.

SOC2 – Created for CSP and IT managed services. It is based on 5 trust principles

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

SOC3 – Similar to SOC2 but for a general audience without disclosing sensitive information.

NIST (SP) 800-53 – Primary goal and objective are to ensure appropriate security requirements and security controls are applied to all US Federal Government.

PCI DSS – Organization which deals with card information should be compliant with PCI DSS.

Merchant Level	**Description (transaction)**
1	6 million and above
2	1-6 million
3	20,000 – 1 million
4	Less than 20,000

System and Sub-system Product Certification

Evaluate claims made for the systems and their components.

Common Criteria: ISO|IEC 15408

Key Components:

- Protection Profile: Defined a standard set of security requirement for a product such as IDS, Firewall etc.
- The Evaluation Assurance Level (EAL): Undergoing more test does not mean the product is more secure

EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Methodically tested and checked
EAL 4	Methodically tested and reviewed
EAL 5	Semi Formally designed and tested
EAL 6	Semi Formally designed, tested, and verified
EAL 7	Formally designed, tested, and verified

**Father Son Mother, My Small Sweet Family*

Common Criteria Evaluation Process:

1. Protection Profile: What does the customer need?
2. Security Target: Vendor's claim of the security
3. Successful evaluation will certify the product

**Common Criteria looks at certifying the product*

FIPS 140-2: Federal Information Processing Standard, issued by NIST to coordinate standard for cryptography modules covering both hardware and software components for cloud and traditional computing environments.

Goal – Primary goal is to accredit the private vendors for cryptographic products who want to have their solution used in US Government Dept.

FIPS Levels:

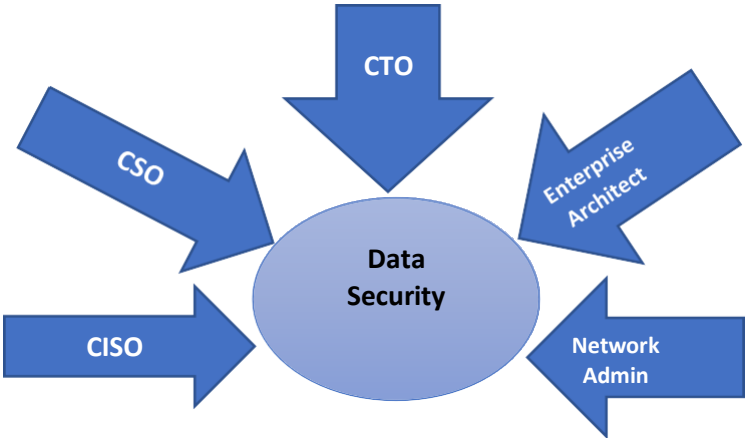
- Level 1: Lowest security. Basic cryptographic requirement. Encryption of the PC board is an example.
- Level 2: Enhances the required physical security mechanism listed in Level 1. Evidence of tampering should prevent unauthorized access to encryption keys.
- Level 3: Develops Level 1 and Level 2 to include the prevention of intruders in the cryptographic module. Should detect access attempts.
- Level 4: Highest rating. Complete protection around the cryptographic module. Detect and respond to unauthorized attempts to physical access. Upon detection, immediate "zeroization" of plaintext critical security parameter.

Exam Essential

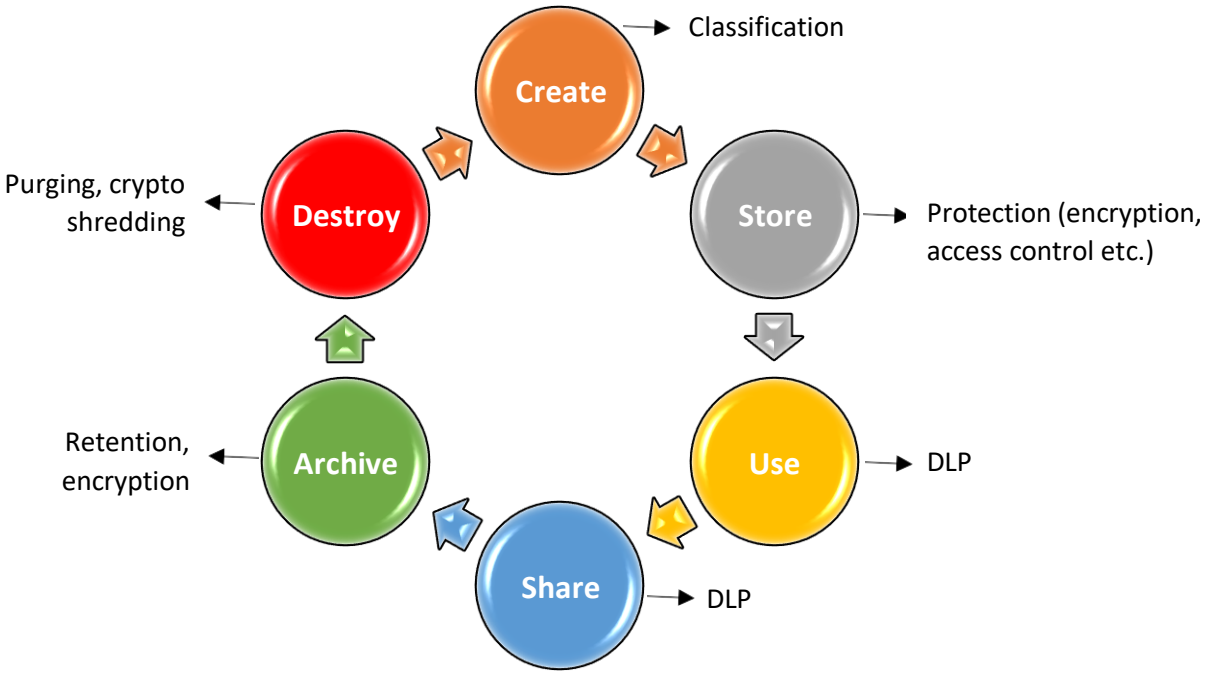
- Roles within Cloud (auditor, service manager, Data architect etc.)
- Building Blocks
- Cloud Reference Architect (Portability, Interoperability, Security, Privacy, SLA/PLA)
- Cloud Deployment Model
- Cloud Services
- Cloud responsibility
- Trusted Platform Module Security
- FIPS 140-2

Domain 2 – Cloud Data Security

In an organization, many roles are responsible for Data security. Few of them are (*but not limited to*):



Data Security Life cycle



**Exam tip: To remember the sequence, use mnemonic (CSUSAD). It also important to understand what happens in which phase of Data Lifecycle*

Lifecycle contains the following steps:

1. Map the different lifecycle phases
2. Integrate the different data locations and access types
3. Map into functions, actors, and controls

Location and Access of data

Location: Data can be generated On-Prem and then moved to cloud and distributed further.

Important questions to ask:

- Who all has access to data?
- What all are potential locations where data needs to be protected?
- What are the controls in each location?
- At what phases of the lifecycle, data moves between location?
- Via, what channels data is moved?
- How are users accessing the data?

Access: Traditional data lifecycle does not specify requirements on who can access the data, from which location, channel etc.

Functions, Actors, and Controls of the data

It is necessary to identify what can be done with the data (***Function***) and who can access the data (***Actors***). Mechanism to restrict access for the people on what action they can perform (***Controls***) e.g. encryption (for confidentiality), Digital Rights Management (for unauthorized access to copyright materials). The controls need to be validated at every point. Controls need to be preventive, detective or corrective.

To determine the necessary controls, the following needs to be clearly identified:

- **Functions** of the data
- **Locations** of the data
- **Actors** upon the data

Key Data Function

Access: View/Accesses the data, including copying, file transfer, and other exchanges of information

Process: Perform a transaction

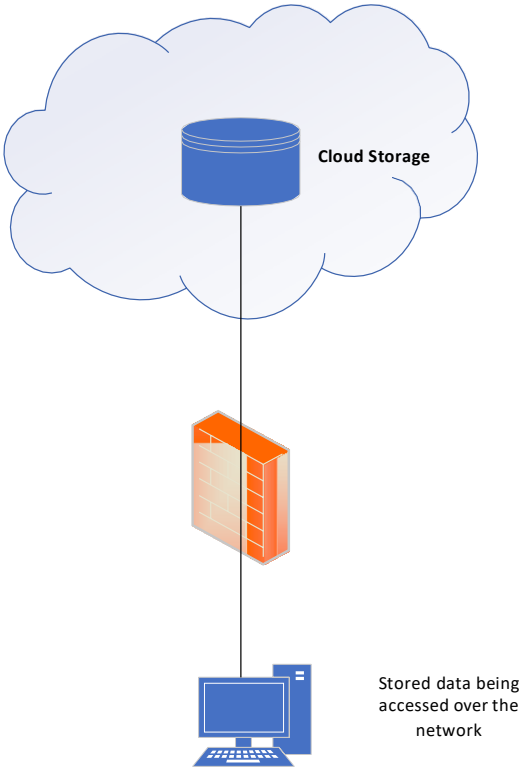
Store: Store the data

	Create	Store	Use	Share	Archive	Destroy
Access	**X**	**X**	**X**	**X**	**X**	**X**
Process	**X**		**X**			
Store		**X**		**X**		

Cloud Services, Products and Solutions

Core of the cloud is software tools with underlying pillars of functionality:

a) Processing data and running applications (Servers)
b) Moving data (Networking)
c) Preserving or storing data (Storage)



Data Storage

Infrastructure as a Service

Consumer	**CSP**
OS	Storage
Software	Network
Host Firewall	Processing

Volume Storage: Virtual Hard drive attached to a virtual machine instance

Object Storage: Similar to file share accessed via API or web interface

Platform as a Service

Consumer	CSP
Application	Infrastructure
Configuration	Network, storage
Data	OS

Structured: Information is stored with high degree of organization which can be found easily (RDBMS)

Unstructured: Not stored in traditional RDBMS. Information such as email, word, text, media content etc.

Software as a Service

Consumer	CSP
Data	Infrastructure
	Network, storage
	OS,Servers, Application

Information Storage and Management: Data entered in system via web UI are stored in SaaS (DATABASE)

Content and File storage: File-based content is stored within application.

Ephemeral storage: Ephemeral means short-lived. For instance, storage; and it exists till the time instance is up.

Content Delivery Network (CDN): Content is stored and distributed to multiple geographical location to improve internet speed.

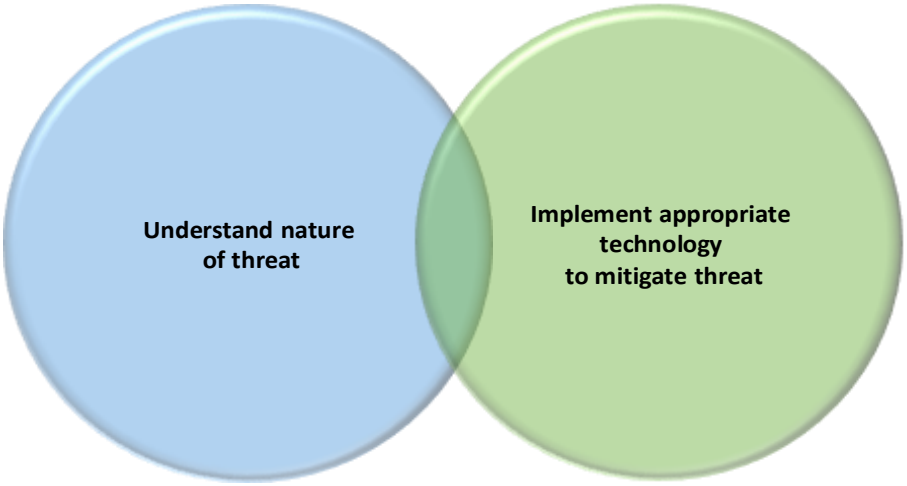
Raw storage: Raw Device Mapping (RDM) is an option in the VMware server that enables storage logical unit number (LUN) to be connected to VM from SAN.

Long-Term storage: Some CSP provides tailored services to store archived data that enterprises can access by using API (**W**rite **O**nce **R**ead **M**any).

Threats to storage types

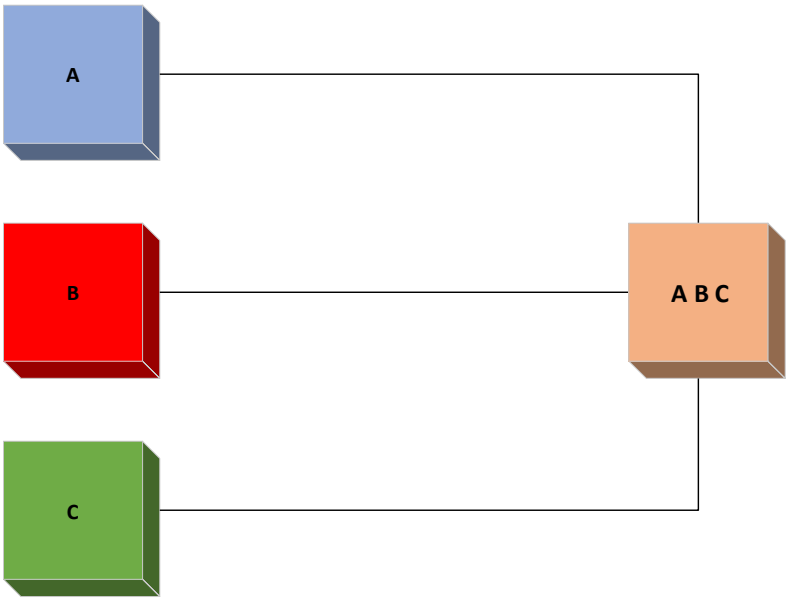
- Unauthorized usage
- Unauthorized access
- Liability due to regulatory non-compliance
- DoS and DDoS attacks
- Corruption, modification, and destruction of data
- Data leakage and breaches
- Theft of accidental loss of media
- Malware attack or introduction
- Improper sanitization after use

Technologies available to address threats



Relevant Data Security Technologies

Data dispersion in cloud storage (*Just like RAID*)



Erasure coding ➔ Chunks data object ➔ into the segment ➔ Segment is encrypted ➔ Cut into slices ➔ Dispersed across all network

Data Loss Prevention

Protects organization's data from standards and policies as well as regulatory requirements.

DLP Components

- Discovery and classification: 1st stage of DLP implementation and an ongoing activity.

- Monitoring: Monitoring for both ingress and egress-based traffic. Cloud-based DLP solution is called as DLP as a Service.
- Enforcement: Includes blocking of data, detect, and alert of breach. It encrypts data prior to leaving the network.

DLP architecture

- Data in Motion: Network-based or gateway DLP. Used for HTTP, HTTPS, FTP, SMTP etc.
- Data at Rest: Looks for data loss on storage.
- Data in Use: DLP is installed on user's workstation and endpoint devices. Challenges are complexity, time, and resources to implement.

Cloud based DLP considerations

- Data in the cloud tends to move and replicate.
- Admin access for enterprise data in the cloud could be tricky.
- DLP technology can affect overall performance.

**Exam tip: Any security control (encryption, DLP etc.) may affect the performance. So, there is a trade-off between the performance and security.*

Encryption

Implementation

- Data in Motion: IPSec, VPN, TLS
- Data at Rest: Retention of data, AES -256
- Data in Use: Data being shared, processed or viewed. Focus on IRM and DRM solution

Cloud encryption challenges

Using encryption should be directly related to business consideration, regulatory requirements and any additional constraints that the organization may have to address.

Different techniques will be used based on the location of data – DIM, DAR or DIU while in cloud.

- Key protection and management
- Software-based key management is vulnerable
- Multi-tenancy is a challenge as resources are shared, and key might be compromised
- Encryption can negatively affect performance
- Encryption in cloud might affect data availability (*if keys are compromised*)

Encryption Architecture

Following components are associated with encryption deployments:

- The data: Object which needs to be encrypted
- Encryption Engine: This performs encryption operation

- Encryption keys: Safeguarding the key is crucial activity

Data encryption in IaaS

In IaaS, encryption encompasses both volume and object storage solutions.

- **Basic storage level encryption:** Encryption engine is located at the management level and CSP holds keys. Protects from the hardware theft or loss. Does not protect from CSP admin accessing the data.
- **Volume storage encryption:** Encrypted data reside on volume storage. Protects against:
    - Physical loss or theft
    - External admins accessing the data
    - Snapshot of storage level backups being taken and removed from the system

Does not protect against access made through the instance or an attack that is manipulating or operating within application on the instance.

Methods to implement volume storage encryption

- **Instance based:** Encryption engine is located in the instance. Keys are managed externally.
- **Proxy based:** Encryption engine running on proxy instance. Proxy instance handles all cryptographic actions.
- **Object storage encryption:** Majority of object storage services offer server-side encryption (*less effective*).

**Encrypt data prior to its arrival to cloud environment.*

External mechanisms include:

- **File level encryption**: Information Right Management (*IRM*) and Digital Right Management (*DRM*) solution. Encryption engine is implemented at client side.
- **Application level encryption**: Encryption engine resides in the application. Encrypts data before reaching to cloud.

Database Encryption

- **File-level encryption:** Encrypting volume or folder of Database with the encryption engine and keys residing on the instance.
- **Transparent encryption:** Database Management System (DATABASEMS) can encrypt entire database or specific tables. Encryption engine resides within database and is transparent to applications.
- **Application-level encryption:** Encryption engine resides at application that is utilizing the database.

Encryption Type	Where the keys reside
File-level	DATABASE Instance
Transparent Data Encryption	Within DATABASE
Application-level	In the application

Key Management

Challenges with key management

- **Access to keys**: Should not be accessible by CSP
- **Key storage**: Secure key storage difficult in cloud
- **Back-up and replication**: It might affect the ability of long- and short-term key management

Key storage in cloud

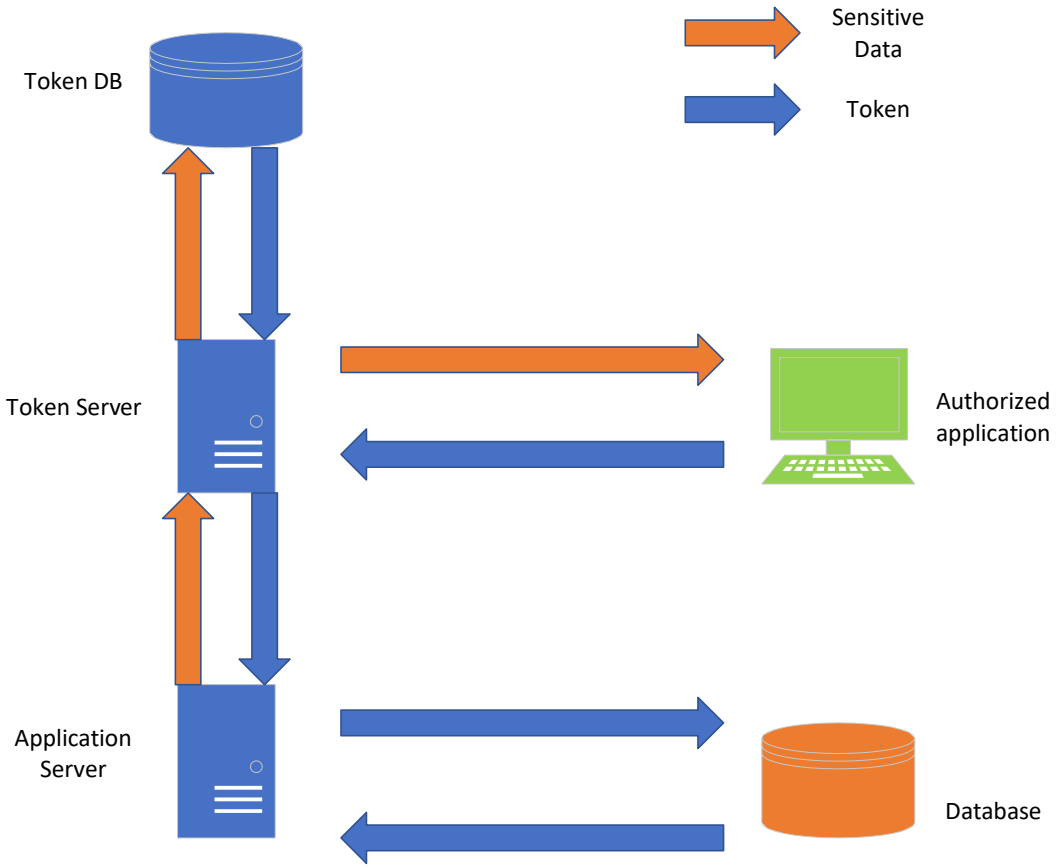
- **Internally managed:** Keys stored on virtual machine or application component used for storage level, internal DATABASE, or back-up application encryption.
- **Externally managed:** Keys are maintained separately from the encryption engine and data.
- **Managed by Third party:** Trusted Third party provides key escrow services. It's important to evaluate the security of Third party storage.

**Software based key management does not meet the physical security requirements specified in NIST, FIPS 140-2 or 140-3*

Masking, Obfuscation, Anonymization and Tokenization

**To protect the confidentiality of data in the cloud (alternative to encryption).*

- **Data masking**: Or Obfuscation is a process of hiding, replacing, or omitting sensitive information e.g. PII, PHI, PCI. It is also used in the test environment to scrub the production or real data and for training purposes. Few common methods are:
    - Random substitution: HELLO ➔ H3!!0
    - Algorithmic substitution: Values are replaced based on an algorithm
    - Shuffle: Shuffles different values from the dataset
    - Masking: 1234 xxxx xxxx 4321
    - Deletion: Simply deletes the data
    - Static: New copy of data is created with the masked values
    - Dynamic: On-the-fly masking. Adds a layer of masking between the application and the database
- **Data Anonymization**: It is a technique for information sanitization with an intent to protect privacy.
    - **Direct Identifier**: Such as Name, e-mail, phone number and other PII (*protected by masking*).
    - **Indirect Identifier**: Such as demographic information, dates, events. (*protected by anonymization*).
- Tokenization: Substituting sensitive information with non-sensitive information



**While storing and retrieving the sensitive data, authentication should be done.*

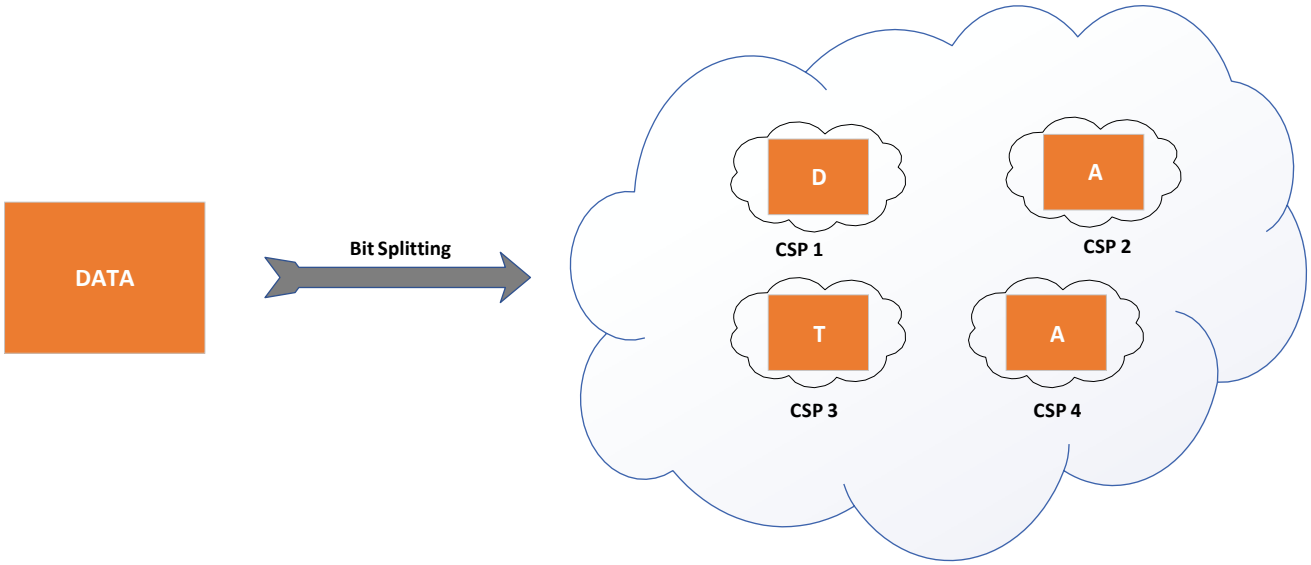
Data Security Strategies

Before creating the strategies, we need to seek an understanding of the following perspective:

- Data type (PII, PHI)
- Data structure and format
- Cloud service module (IaaS, PaaS or SaaS)
- Cloud storage option
- Define data ownership
- Protection of data control
- Ongoing monitoring

Emerging Technologies

1. **Bit Splitting:** Splitting up and storing encrypted information all across the cloud storage.



Single CSP does not have access to all the data

Benefits

- Data security is enhanced
- Makes harder to gain access to data for legal process as data is present in multiple location
- Scalable and prevent vendor lock-in

Challenges

- Processing overhead
- Storage requirement and cost is high
- Availability issues

Methods

- Secret Sharing Made Short (SSMS): It has 3 phases
  - Encryption of Information
  - Use Information Disperse Algorithm (IDA)
  - Using the encryption key using the Secret Sharing Algorithm
- All or nothing transformation with Reed Solomon (AONT-RS): Integrates AONT and erasure coding:
  - Encrypts and transform information and encryption key into blocks.
  - Uses IDA to split blocks in *'m'* shares, which is distributed to different cloud share

2. **Homo-morphic Encryption:** It enables processing of encrypted data without the decrypting it. As its still developing technology, only small amount of data is encrypted using this technique.

Data Discovery

Goal of data discovery is to find out meaningful data. There are various approaches for this technique few of them are:

- **Big data**: Depends on Volume, Variety, and Velocity of data. The high volume of data makes it challenging.
- **Real-time analysis**: Discovery is performed more often and in more diverse ways. Needs to have more fast tools.
- **Agile analytics and Agile business intelligence**: Follow agile methodology of data discovery. Creates new class of use cases for data discovery.

Different data discovery techniques

- **Metadata:** It is data that provides information about another data. *(Data about data).*
- **Labels:** Marking that describes the data.
- **Content Analysis:** Data is analyzed by the pattern matching, hashing, statistical etc. e.g. Luhn check or Mod10 formula to find any 16-digit number is valid credit card number or not.

Data discovery issues

- **Poor data quality:** Data visualization is as good as the amount and quality of data being fed.
- **Dashboards:** Data present in the dashboard is not always accurate to rely upon. It also has security issues.
- **Hidden cost:** Hiring the right skilled people for business intelligence.

Challenges of data discovery in cloud

- Identifying where your data is?
- Accessing the data. Not all data stored in cloud could be accessed by everyone.
- Data preservation needs to be decided between customers and CSP in the contract.

Data Classification

To classify data, it is crucial we understand –

- What are the data types?
- Where is the data located?
- What are access levels implemented?
- What is the protection level, compliance?

Data Labeling – Tagging data with additional information (Department, location, classification etc.) *Classification is a part of data labeling.*

Challenges with cloud data

- **Data creation:** Data must be classified at the time of creation.
- **Classification control:** Preventive, administrative, and compensating control.
- **Metadata:** Classification should also be done based on metadata.
- **Classification data transformation:** Data or metadata should be preserved in case of data format change.

- **Reclassification consideration:** Reclassification must be supported. If the classification is increased, controls should be implemented.

Data Privacy Act

Privacy and Data Protection (P&DP): It affects data subject (*people*) and cloud customers (*organization*).

Global P&DP Laws in US: US doesn't have official privacy data protection authority. Federated Trade Commission has jurisdiction over most commercial entities. 4th amendment protects from searches and seizures.

Global P&DP Laws in EU: EU Directive 95/46/EE. Privacy of EU citizens and their personal data being used.

Global P&DP Laws in APEC: Develop effective privacy protection that avoid barrier to information flow, ensures continued trade. (*flexible*)

Applicable law: The law which is applicable for a case. It determines legal standing of a case or issue.

Jurisdiction: It determines the ability of a national court to decide a case or enforce a judgement or order.

**Ultimate foal of P&DP law is to provide safeguards to data subject for processing of personal data.*

Common Privacy terms

- **Data subject:** Subject who can be identified directly/indirectly.
- **Personal Data:** PII, PHI, payroll data, etc.
- **Processing:** Operation on data (collection, processing).
- **Controller:** Person or entity which decides what needs to be done with data (*e.g. your organization collecting employee information*).
- **Processor:** Processes the data on behalf of controller (*e.g., your organization outsources the payroll processing to Third party, that Third party becomes the processor*).

**In the contractual agreement, privacy roles like who is a controller and who is a processor should be clearly specified.*

Responsibility depending on type of cloud services

Responsibility per cloud service model	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
GRC (Security Governance, Risk & Compliance)			
Data Security			
Application Security			
Platform Security			
Infrastructure Security			
Physical Security			

Customer Responsibility

Shared Responsibility

Provider Responsibility

**In SaaS and PaaS, CSP can also be controller or joint controller with customer.*

Implementation of data discovery

- **From the customer's perspective:** The customer as a controller has full responsibility of compliance, discovery, classification, and adherence to P&DP law.
- **From the service provider's perspective:** CSP should be able to demonstrate the implementation of security controls as a processor.

Classification of discovered sensitive data

- **Scope and purpose of the processing:** Processing of administrative data would have fewer security controls than the processing of payment details of customers.
- **Categories of the personal data to be processed:** What are the data types that will be processed?
    - Personal Data
    - Sensitive data (health, sexuality)
    - Biometric data

  Operation on these data:

    - Collection
    - Selection
    - Erasure
    - Recovering
    - Retrieval
    - Organization
    - Comparison
- **Categories of users allowed:** Access to the data should be given based on the user's role (*RBAC*)

- **Data retention constraints:** The majority of the data processed should be retained *(and then purged*).
- **Security measures to be ensured:** Type of security depends on the purpose and data to be processed.
- **Data breach constraint:** Several P&DP laws provides an obligation to report to concerned people after a breach has happened.
- **Status:** After a breach, what is the current state of data?

**Key privacy cloud service factors stem from the "Opinion 5/2012 on cloud computing" adopted by WP29.*

Privacy Level Agreement

The CSP declares the personal data protection and security that it sustains for the relevant data processing. It does the following:

- CSP communicated the level of protection is offered
- Access the level of compliance for CSP
- Provides contractual protection

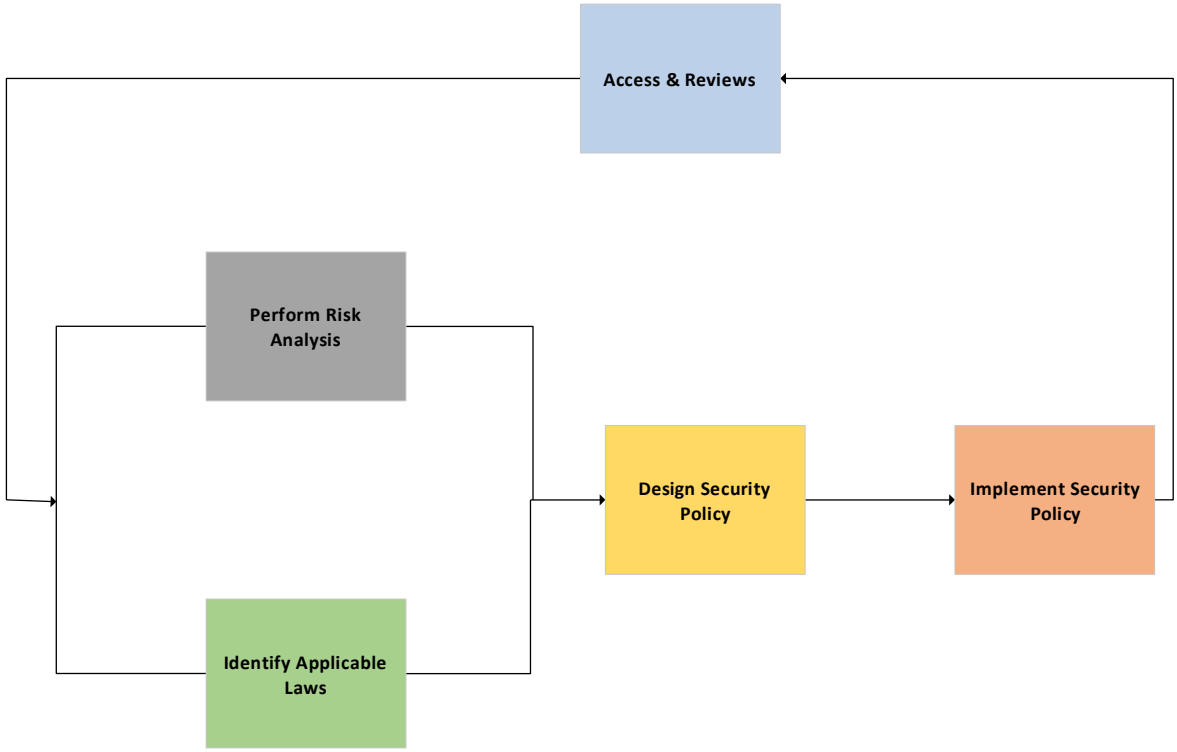
Application of defined controls for PII

Trust services principles and criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP100) that AICPA has developed.

Principles to be used in Trust Service Engagement:

- **Security**: The system is protected against unauthorized access (Physical and Logical).
- **Availability**: The system is always available.
- **Processing Integrity**: System processing is complete, accurate, timely, and authorized.
- **Confidentiality**: Confidential information is protected as agreed.
- **Privacy**: Personal information is collected, processed and destroyed as per Generally Accepted Privacy Principles.

Management Control for Privacy and Data Protection measures



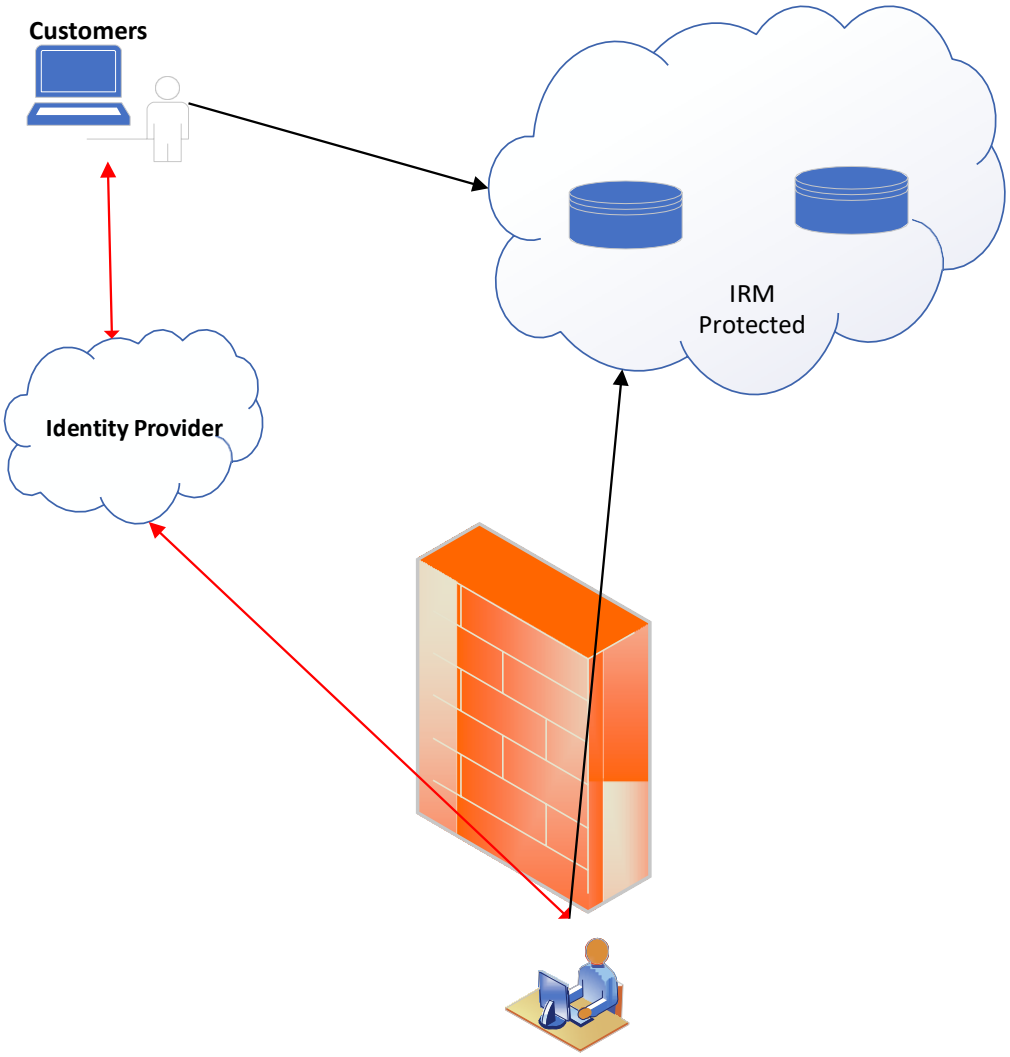
Management oversight is important

Data rights management objectives

Features of Information Rights Management (IRM)

- Adds an extra layer of access control (ACL)
- As IRM has ACL, controls are independent of file location
- IRM can be used to protect various documents
- It can be used as a baseline for default information protection

IRM Cloud challenges (**Each user should have the matching encryption keys. Need a strong Identity Infrastructure*)



- Should have Role-Based Access Control (RBAC)
- It can have a federated identity
- IRM agent installation limit external users to access the IRM content
- Compatibility issues with reading software
- Compatibility issues with OS when used in mobile devices
- It can be integrated with DLP tools

IRM solutions

- **Persistent Protection:** Everything is protected at rest and in transit
- **Dynamic Policy control:** Allows content owners to define and change user permission or even expire the content.
- **Automatic Expiration:** Automatically revokes access.
- **Continuous audit trail:** Ensuring delivery of the message content.
- **Authentication:** Support for existing authentication security infrastructure.
- **Mapping for repository ACL:** Automatically maps the ACL-based permissions into policies that control the content outside the repository.

- **Integration support:** Integration with all Third party email filtering engines.
- **Additional security and protection capabilities:** Determining access control, least privilege, logging, and monitoring.
- **Support for email applications:** Support for tools like Outlook, Lotus etc. and other document types.

Data protection policies

- **Data retention policies:** It's a regulatory and business requirement. Should have the following:
  - Retention period
  - Data formats
  - Data security
  - Data retrieval procedures for the enterprise
- **Retention policy for cloud:** Legislation, regulation, and standard requirements.
- **Data mapping:** Process of mapping data type (structured and unstructured), data formats, file types, and data location.
- **Data classification:** Classification is used to determine the retention period.
- **Data retention procedure:** Back-up and retrieval options, restore procedures.
- **Monitoring and maintenance:** To ensure the entire process is working properly.

Legal Hold

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a legal hold to ensure the preservation of relevant documents.

Data deletion procedures and mechanisms

Safe disposal of data is needed to ensure no data remanence. Various available options for sanitization includes:

- Physical destruction
- Degaussing
- Overwriting
- Encryption

Crypto shredding: The process of encrypting the data to dispose of is called digital shredding or crypto shredding. Once the data is encrypted, keys are destroyed. Few important points should be taken into consideration as a part of the crypto shredding process:

- Data should be completely encrypted without leaving any clear text.
- Encryption keys are completely unrecoverable. This is difficult if keys are managed by CSP.

Data archiving procedures and mechanisms

Archiving for cloud should contain the following elements:

- **Data encryption procedure:** Key management should be handled properly.

- **Data Monitoring Procedures:** Security controls should be implemented throughout the data lifecycle.
- **Ability to perform e-discovery and granular retrieval:** We should be able to perform e-discovery to determine which data should be retrieved.
- **Back-up and DR option:** It's Important that BCP/DR procedure is aligned to the organization's policy.
- **Data format and media type:** Archiving data should be done in the right format to ensure storage management is properly done.
- **Data reservation procedures:** Data should be restored periodically and in an isolated environment.

Events

All the events should be centrally logged and monitored using SIEM technology.

- SaaS event sources (*no control of customers*):
  - Web server logs
  - Application server logs
  - Database logs
  - Guest OS logs
  - Host access logs
  - Virtual logs
  - Network captures
  - Billing records

**Exam tip: Document the access to log data in the contractual agreement with CSP*

- PaaS event sources (*some control to customer*):
  - Input validation failures
  - Authentication success and failures
  - Authorization failures
  - Session management failures
  - High-risk functionality (e.g., privileged user access, network connection, key exchanges)
  - Legal and other opt-ins

- IaaS event sources (*customer has control of data*):
  - Cloud network logs
  - DNS server logs
  - VM logs
  - Host OS and Hypervisor logs
  - API access logs
  - Management portal logs
  - Packet captures
  - Billing records

Identifying Event attributes requirement

WHEN

- Log data and time (International format and Network time protocol)

- Event date and time (Timestamp)

WHERE

- Application identifier
- Geolocation
- Code location

WHAT

- Type of event
- Severity of event
- Description

Additional details: Reason, secondary time source, HTTP code.

**Exam tip: Preservation is defined by ISO 27037:2012. It draws the process to maintain and safeguard digital evidence.*

Security Information and Event Management (SIEM)

Security Information Management + Security Event Management = SIEM

(*Storage, analysis, and reporting*) (*Real-time monitoring, correlation, and notification*)

- Data Aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic Analysis

Supporting continuous operation

- Audit logging
  - New event detection
  - Adding new rules
  - Reduction of false positive
- Contract and authority maintenance
- Secure disposal (crypto shredding)
- Incident response for legal preparation

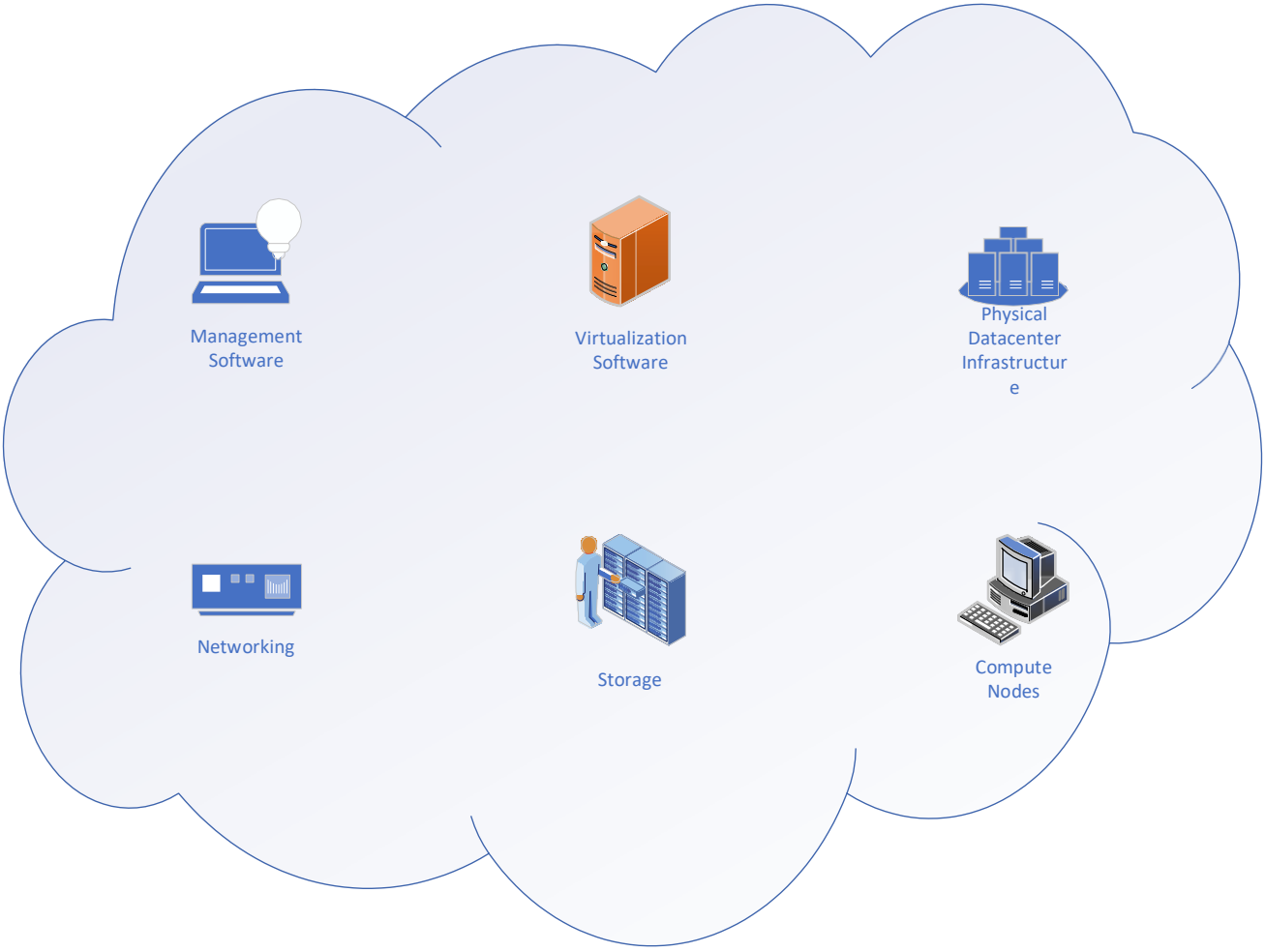
Chain of custody and non-repudiation

Chain of custody is the preservation and protection of evidence from the time it was collected and it was presented to the court. Any break in the chain of custody makes the evidence inadmissible in the court.

Exam Essential

- Data lifecycle
- Different Storage
- Different encryption (Side-Channel Attack)
- Key Management (Key and data should not be stored in the same location)
- IRM/DRM

Domain 3 - Cloud Platform and Infrastructure Security

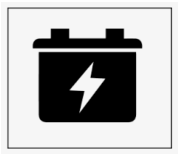


Cloud Infrastructure

CSP can provide multiple levels of services. Basic is called power (electricity), pipe (connection) and ping (Remote access internet).

Given low tolerance to failure, a Datacenter should be chosen considering geographical and political risk.

Datacenter design



Back up Power

Multiple entry points for power and network

Multiple Cooling units

Redundancy

Multiple building entrances

Multiple Power lines

Multiple Power Distribution Units

No single point of failure

Network and Communication in the Cloud

The purpose of the network is to provide control communication between services and clients.

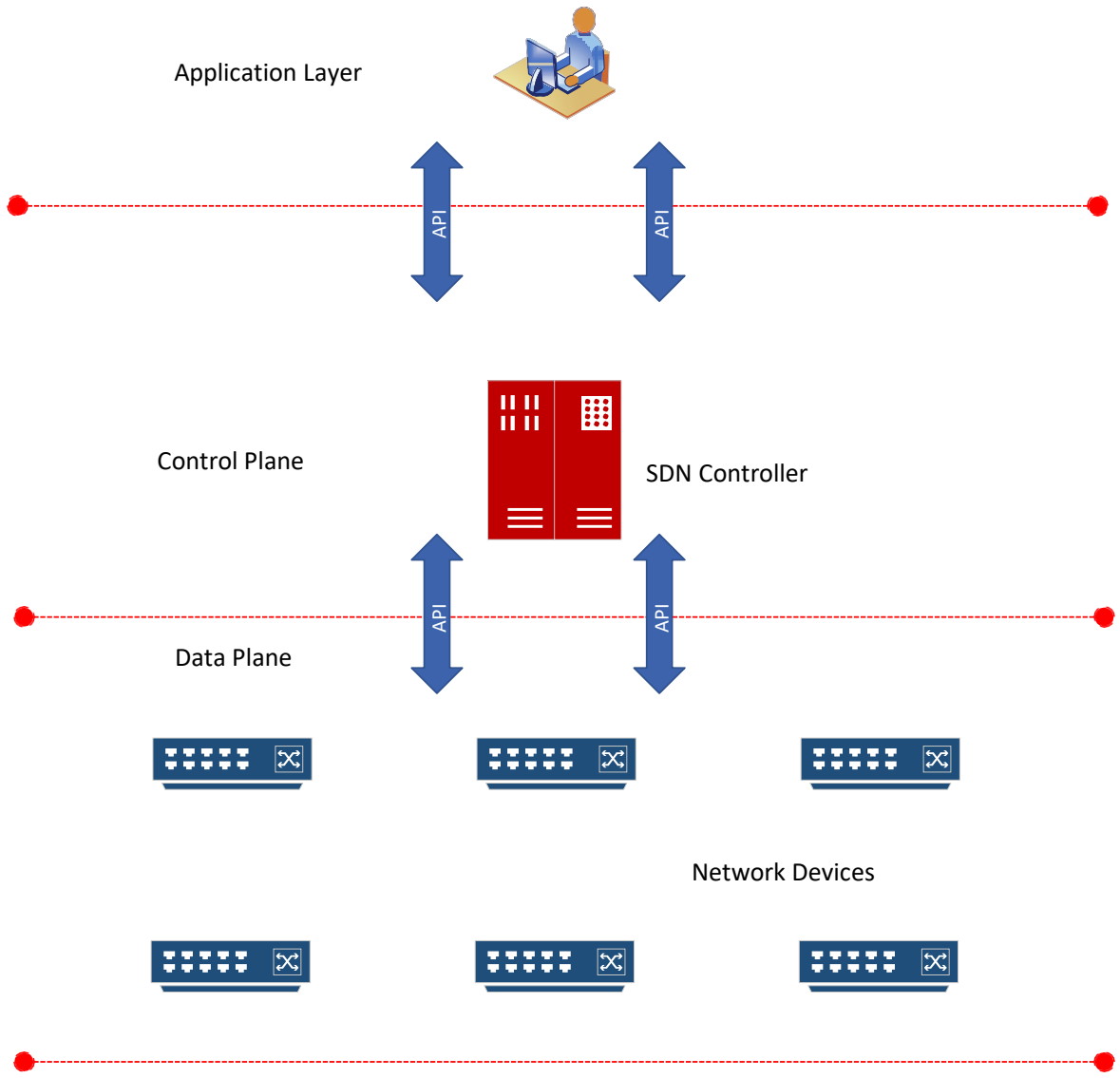
- **Cloud Service Consumer:** Person or organization who uses services from CSP.
- **Cloud Service Provider:** Responsible for making services available for consumers.
- **Cloud Carrier:** The intermediary that provides connectivity and transport of cloud services between the CSP and consumer.

Network Functionality

- **Address Allocation:** Should be able to provide one or more IP address to a cloud resource (static or dynamic)

- **Access Control:** Mechanism used to grant or deny access to a resource
- **Bandwidth Allocation:** Specific amount of bandwidth provided for the system to use
- **Rate Limiting:** Ability to control the amount of traffic and API
- **Filtering:** Ability to selectively allow or deny content
- **Routing:** The ability to direct the flow of traffic between endpoints based on the best path

Software-Defined Networking (SDN): Decouple Control plane and Data (Forwarding) Plane



SDN Architecture

The Compute Parameters of a Cloud Server:

- Number of CPU's
- Amount of RAM Memory

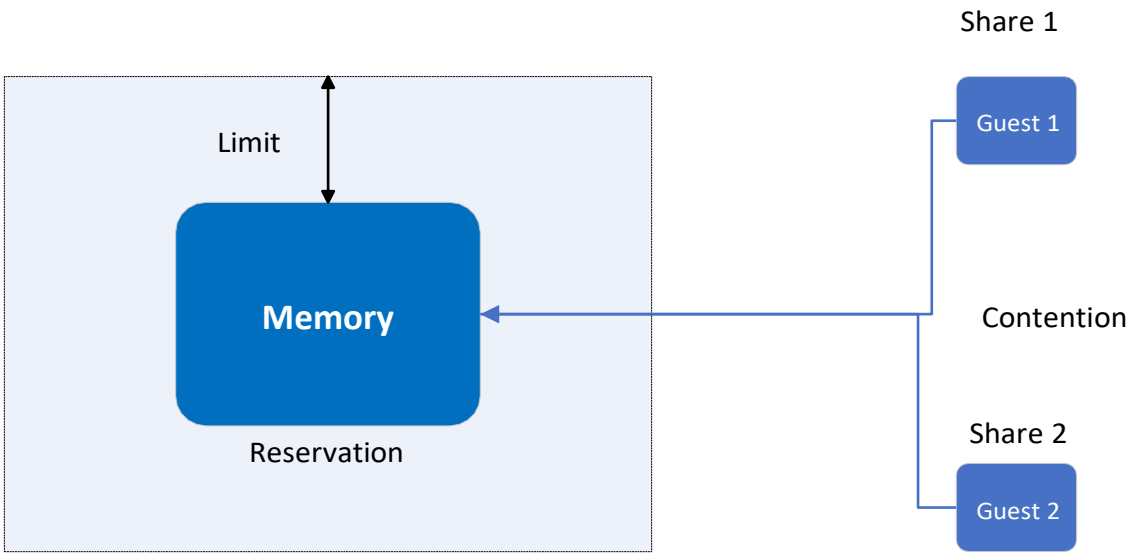
Compute resources of a host is the ability to manage and allocate these resources effectively either on 1) per guest OS basis 2) per-host basis

Reservation, limit, shares help an administrator to allocate compute resources of a host.

Reservation: It guarantees minimum resource allocation. It's either available for CPU or RAM or both.

Limit: It creates a maximum ceiling for resource allocation. It can be fixed or expandable.

Share: It is to manage issues with computer resources during a contention situation. Example, A lot of requests are placed for limited available resources. Share number gives priority to the guests who are making requests and accordingly resources are allocated.



Reservation, Limit and Contention

Virtualization: It makes cloud computing possible

- **Scalability:** Multiple guest OS can be run. Guest is an isolated software instance that runs on a hypervisor.
- **The Hypervisor:** Piece of hardware, software, or Firmware gives Guest OS's an impression that they are running on Physical Hardware.

**VMM (Virtual Machine Manager) is used to create one-to-one instance between Hypervisor and VM.*

Type 1 Hypervisor

- Called as Bare Metal, embedded, native hypervisor

- Works on hardware and can monitor Guest OS
- Small because they share and manage hardware resources between different Guest OS

Type 2 Hypervisor

- Installed on top of Host OS and dependent on Host OS for its operation

Risk and Challenges:

- Security flaws in hypervisor can lead to malicious software targeting individual VMs running on it
- Flawed Hypervisor can facilitate inter VM attacks (aka VM hopping) when VM isolation has not been configured properly
- Network traffic between VMs is not visible, which means additional control is needed
- Resource availability for VMs can be flawed. VM can be starved of resources
- VMs and their disk images are files residing somewhere else. So, a stopped VM can be accessible by Third party if no proper controls are applied

Storage issues in the Cloud:

Resistant mass storage in Cloud is by spinning hard disk drives of solid-state drives (SSD)

**For redundancy: RAID*

Logical Unit Numbers (LUN): Group disks are sliced up into logical volumes of arbitrary sizes.

- **Object Storage (***file, stored in metadata***):**
    - CSP provides a file system like a scheme to its customer
    - Objects are accessed through API (Web UI) e.g. Amazon S3 and Rackspace Cloud Files
    - Object Storage is used to store OS images; it increases resilience and provides redundancy

****Data consistency is achieved eventually, e.g. change is propagated after some time.*

***Not suitable for data that changes frequently*

**Suitable for backups, archives, video and audio files, and VM images*

- **Management Plane:** Allows admin to manage any or all of the hosts remotely.

Key Functionality: Create, start and stop VM instance, and provision them with virtual resources like CPU, memory, etc.

**Exam tip: As its most powerful tool, it integrates authentication, access contro,l and logging and monitoring of resources used. If the Management Plane is compromised, it can bring down the whole infrastructure.*

It's used by privileged users who install and remove hardware, software, firmware. The primary interface is API.

**APIs allow automation of controls tasks.*

Management of Cloud Computing Risks

Enterprise Risk Management is a set of process and structure to systematically manage all risk to the enterprise, explicitly supply chain and Third party risks.

**Exam tip: In the end, customer and CSP is responsible for its own risk assessment.*

Policy and Organization Risks: Related to choices that consumer makes about CSP

- Provider lock-in: High cost in switching between providers
- Loss of governance: Consumer not implementing all the controls
- Compliance Risks: Specific CSP may not be compliant with all regulations like HIPAA, PCI, etc.
- Provider exit: Bankruptcy of CSP

General Risk: Potential failure to meet any performance, operability, security, etc.

- Single Point of failure
- More skills needed by CSP for a larger platform
- Control over technical risk shifts to CSP

Virtualization Risk

- Guest Breakout: Guest OS can access hypervisor or the Guest OS
- Snapshot and Image Security: It contains sensitive information which needs to be protected
- Sprawl: Loose control of the amount of content on your image store

Cloud Specific Risk

- Management Plane Breach: If compromised, the entire infrastructure can be affected.
- Resource Exhaustion: Considering resources are shared in the cloud environment, exhaustion is a risk to customers. Can cause DOS, traffic analysis, manipulation or interception of data.
- Isolation Control Failure: CSP with multiple tenants need to have proper resource isolation.
- Insecure of incomplete data deletion: Risk of data remanence and reusability of storage can lead to sensitive data exposure.
- Control Conflict Risk: Controls more secure for (Block Traffic) - One tenant makes it less secure for the tenant (loss of visibility).
- Software related risks: Potential vulnerabilities on the software being run in the cloud environment by CSP.

Legal Risk

- Data Protection: Protection of PII and other sensitive data by CSP.
- Jurisdiction: Data storage in multiple location, in multiple jurisdiction which can affect risks and control.
- Law Enforcement: If law enforcement asks for data, its hard for CSP as it may lead to exposure of data of other tenants.
- Licensing: Moving licensed software from on-prem to cloud.

Non-Cloud specific risks:

- Natural disaster, unauthorized facility access, social engineering, network attack, etc.

Cloud Attack Vectors:

- Guest Breakout
- Identity compromise
- API compromise
- Attacks on the provider's infrastructure and facilities
- Attack on connecting infrastructure (Cloud carrier)

Countermeasure Strategies Across the Cloud

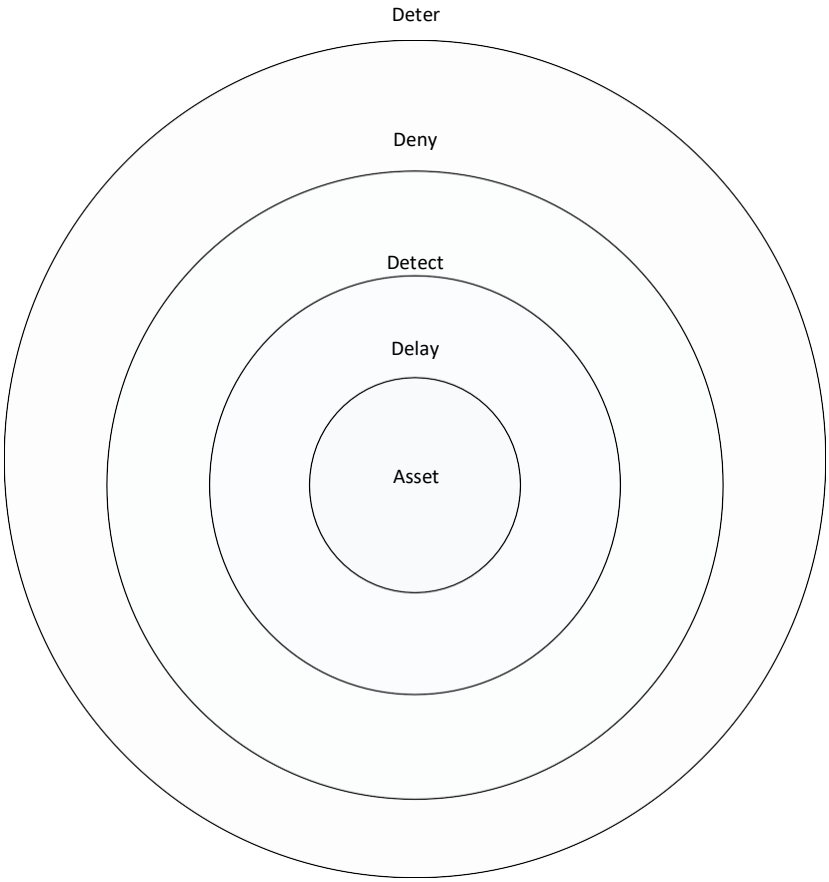
- Defense in Depth
- Multiple Controls (compensating control)
    - Intent and rigor of the original environment
    - Provide a similar level of defense
    - Be above and beyond other requirements
    - Commensurate (proportionate) with additional risk
- **Continuous Uptime:** Makes it resilient and redundant
- **Automation of Controls:** Helps in immediate and comprehensive implementation
- **Access Controls:** Depending on the model, responsibility may lie with the consumer, CSP, or both.
    - Building Access
    - Computer floor Access
    - Access to physical servers, racks, etc.
    - Hypervisor, Guest OS access
    - Developer, customer, vendor and remote access
    - Strong authentication and Identity Management

Physical and Environmental Protection ***(****Datacenter, buildings and its surroundings)*

**NERC CIP: Set of requirements designed to secure the assets required for operating North Americabulk electric system (9 standards and 45 requirements).*

- Key Regulations**:** HIPAA, PCIDSS
- Examples of Controls:
    - Policies and procedures for a safe work environment
    - Physical access to information asset should be restricted
    - Physical security perimeter should be placed

- Protecting Data Centre Facilities



Layered Defense

System and communication Protections

Identify critical assets, trace the flow across components and map out relevant controls. Cloud still runs on the hardware. These need to be protected, properly configured, maintained, and analyzed for risk.

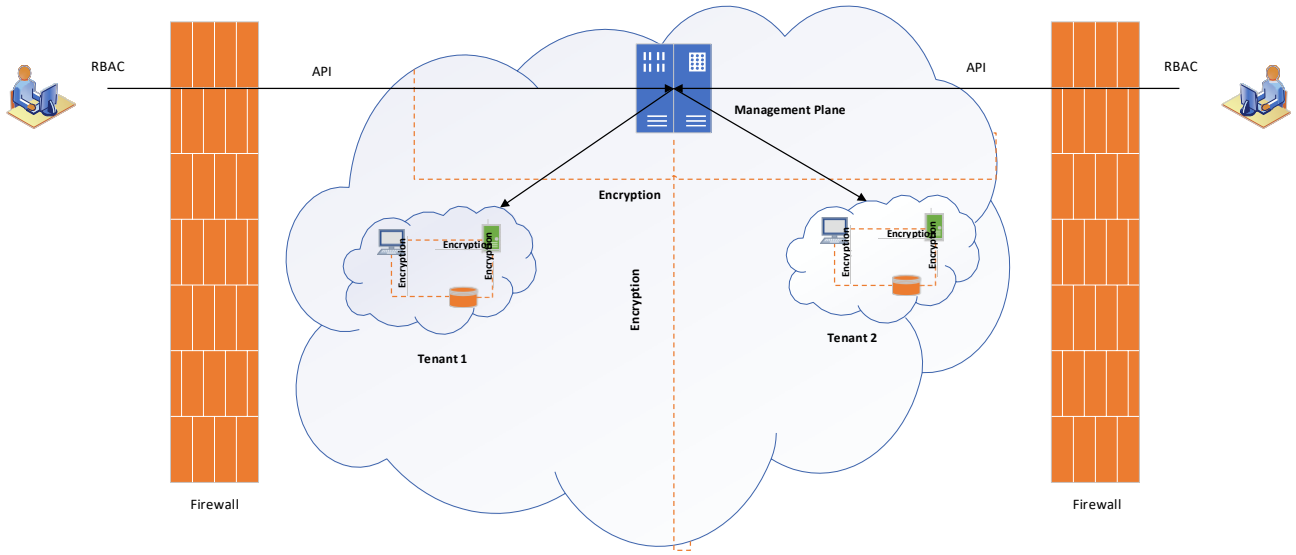
- **Automation of configuration:** It's easy, error-free, provides more granular proliferation (growth) of controls.
- **Responsibilities for protecting the cloud system**

Responsibility per cloud service model	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
GRC (Security Governance, Risk & Compliance)			
Data Security			
Application Security			
Platform Security			
Infrastructure Security			
Physical Security			

Customer Responsibility
Shared Responsibility
Provider Responsibility

- **Following the Data Life cycle**
  - **DAR:** Encryption at rest, store at multiple storages for availability
  - **DIM:** Logical and Physical Segmentation. Data in transit encryption, layered architecture
  - **DIU:** API should be encrypted and digitally signed. API should be authenticated and authorized.

Virtualization Systems Controls: Virtualization components are compute, storage and network all governed by the management plane.



- Management Plane manages the entire infrastructure of cloud. Part of it is exposed to customers to manage their operations.
- APIs should have stringent RBAC.

- Logging is also important. Capacity monitoring, isolation, IDS, IPS.
- Trust Zone (separate classification) - Confidentiality
- Capacity and Risk – Availability

Virtualization infrastructure enables

- Traffic isolation
- Guest security (IaaS consumer)
- File and volume encryption
- Control and image provenance (*create, distribute, store, use, retrieve, destroy*)

Managing Identification, Authentication, and Authorization in the Cloud Infrastructure

Anything that needs to be trusted has an identity.

**MFA for Admin Authentication*

Authorization on Federated domain happens at Relying party. Accounting for resource is done by logging, monitoring the amount of time, and system resources consumed.

*Access Decisions are made using Policy Enforcement Point (PEPs)

*Individual policies are controlled at Policy Decision Point (PDP)

Entitlement Process:

Users are entitled with the access rights which they are allowed to perform.

Risk Audit Mechanism:

The purpose of risk audit is to provide reasonable assurance that adequate risk controls exist and are operationally effective.

The Cloud Security Alliance Cloud Control Matrix: Framework for cooperation between CSP and consumers.

Using a VM

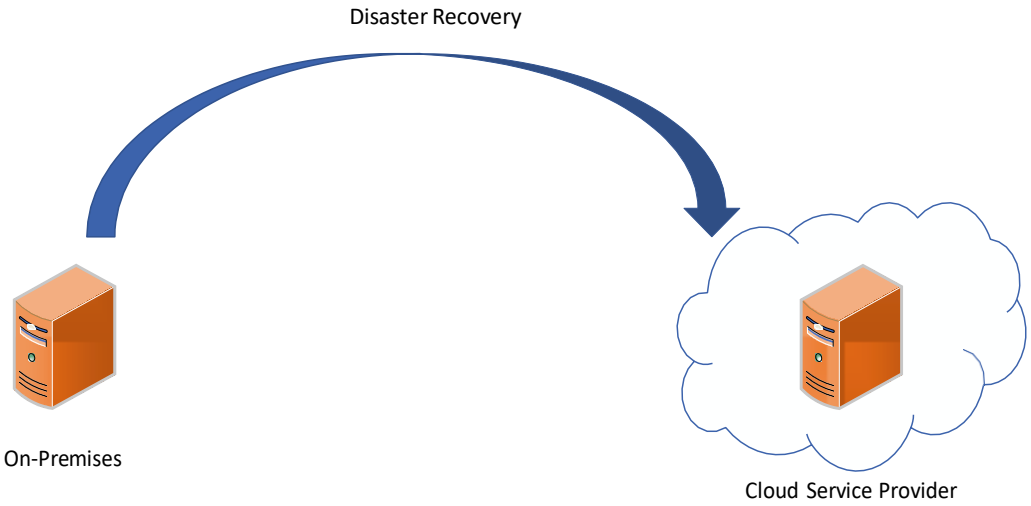
Creates a baseline for VM image and can provide evidence for adequate security control. In Cloud Computing, automation and self-service provisioning can be progressed to lead the continuous auditing. The existence effectiveness of controls are tested and demonstrated on a continuous and on a real-time basis.

Understanding the Cloud Environment Related to BCP and DR (BCDR)

BCP: Allows a business Plan decide what it needs, to ensure that its key products and services continue to be delivered in case of Disaster.

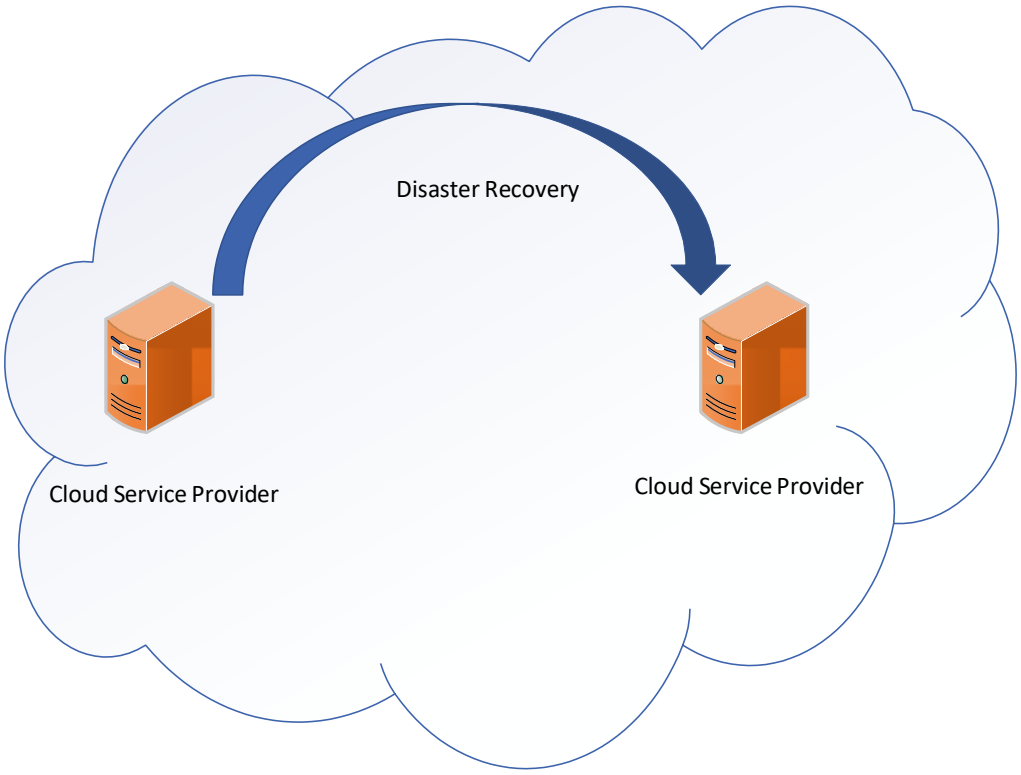
DR: Allows business to plan what needs to be done immediately after a disaster to recover from the event

On-Premises, Cloud as BCDR



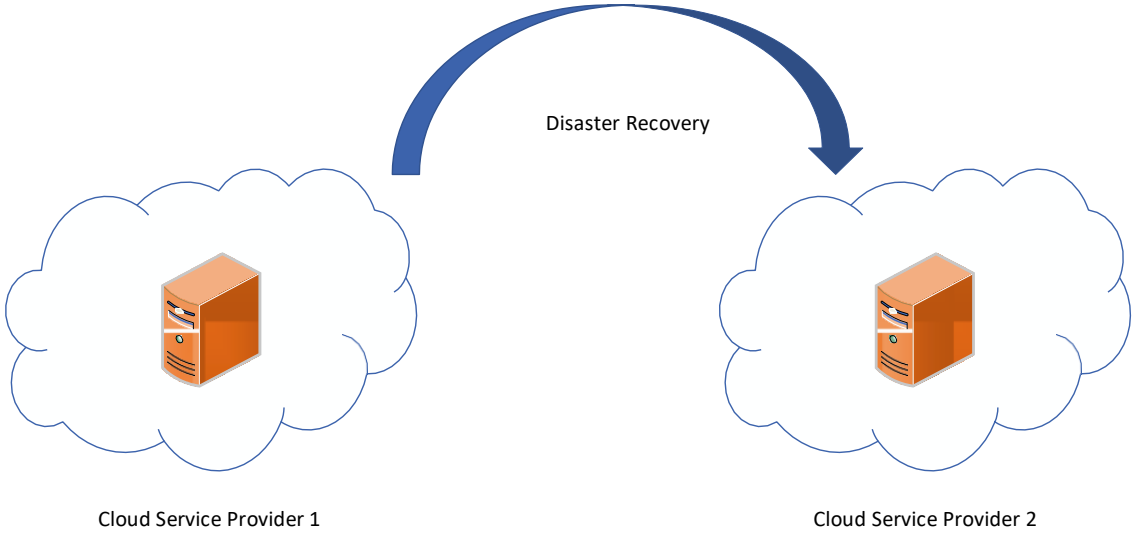
CSP serves as endpoint for failover services

Cloud Consumer, Primary Provider BCDR



One region fails, service is restored in another zone of Cloud

Cloud Consumer, Alternative Provider BCDR



Failure happens, restoration happens in another location

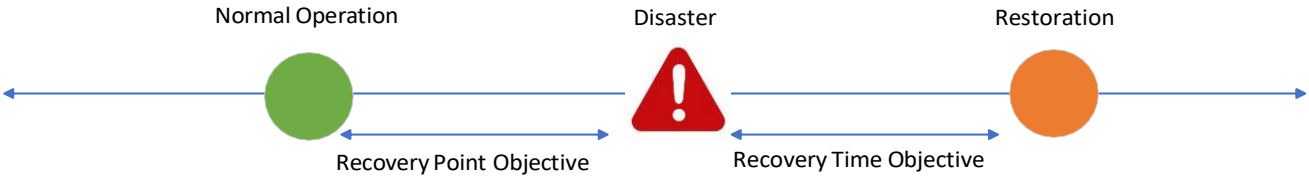
BCDR Planning Factors

- Important Assets: Data and Processing
- Current location of the assets
- The networks between the assets and the sides of their processing
- Actual and potential location of the workforce and business partners concerning disaster event

**Cloud has resilient infrastructure, broad network connectivity and can be quickly deployed.*

**Its pay per use, which means BCDR can be a lot cheaper*

Understanding the Business Requirement related to BCDR



RSL (Recovery Service Level): Percentage measurement (0-100%) of how much computing power is necessary based on the percentage of production system needed during a disaster

e.g., Critical systems = 5 system

**During disaster, percentage of computing power needed to run 5 systems.*

Understanding the BCDR risks

**Risk to assets and support infrastructure*
**Risk to BCDR execution plan*

- **BCDR risk requiring protection:** Flood, earthquake, etc. wear and tear of equipment service outage and other failures.

- **BCDR Strategy Risks:** Risks which are intrinsic (Built-in or internal) to BCDR strategy:

    - Complicated architecture due to redundancy
    - Failure of failover device/cluster
    - The off-site location being too remote can cause latency issues.Regulatory compliance of off-site in a different jurisdiction.

- **Potential concerns about BCDR scenarios:**

    - Existing on-prem solution using Cloud as BCDR
    - Existing consumer evaluating their CSP: BCDR
    - Existing consumer evaluating alternative CSP as BCDR

BCDR Strategies

It is important to consider an alternative for every solution in an account of a disaster.

- **Location:** Choose a location in a way that offsite should not be affected by the same disaster.
  **Switching CSP also provides BCDR*

- **Data Replication:** Can be replicated at the block level, file level, and database level. Can be replicated in bulk, byte, database mirroring—daily shipping dependency on RPO and other recovery strategies.
  **Block level data protects against physical data loss but not against database corruption*
  **While choosing data replication strategy, storage and bandwidth should be considered*

- **Functionality replication:** Replicating or recreating the processing capacity on a different location.
  **In SaaS, it might be needed to choose a different CSP*

**Situation where the existing environment is majorly virtual, it would be easy to recreate the processing capacity*

- **Planning, Preparing and Provisioning:** It's about tooling, functionality and processes
  **Sooner the anomaly is identified during failover, lesser would be RTO*

- **Failover Capability:** Load balancers to re-direct user's service requests.

- **Returning to normal:** In case of temporary failure, returning to primary provider/service / site should be done (Failback)

Creating the BCDR Plan

- **Scope of the BCDR Plan**: BCDR should be considered as an intrinsic part of IT services that are regularly invoked (only for testing purpose).

- **Gathering Requirements and Context**: Find out critical business functions and assets. Business strategy influence RTO and RPO.

- **Analysis of the Plan**: The purpose of this phase is to translate BCDR requirements into input to be used in the design phase.

- **Risk Assessment**: BCDR should be assessed for any residual risk.

- **Plan Design:** Objective into establishing and evaluate candidate architecture solution. This phase should give not only technical alternative but also procedures and workflows.

- **Other Plan considerations:** Once the design is ready, implementation will begin.

- **Planning, Exercising, Assessing, and Monitoring the plan:** Once the plan has been implemented, it is important to test the plan.

**Exam tip: BCP should be tested at least annually*

Integrated testing goes beyond the testing of individual components to include testing with internal and external parties. Organizations should periodically re-assess and update their test scenarios to reflect changes in the organizations business and operating environments

- **Test Plan Review:** Test plan should be reviewed before testing.
  - **Checklist review:** Distributing copies of BCP to managers of each critical business unit asking them to review.
  - **Tabletop Exercise / Walk Through Test:** Primary objective is to ensure that critical personnel are aware of BCP and plan accurately reflects the organization's ability to recover from disaster.
  - **Walk Through Drill / Simulation Test:** More involved than tabletop. Participant choose a specific scenario and apply BCP to it.

- **Functional Drill / Parallel Test:** People move to an offsite location to see if BCP is properly invoked.
- **Full interruption Test / Full scale Test:** Primary site is stopped and actual BCP is invoked.

- **Testing and Acceptance to Production:** Once the plan is tested, it should be documented, periodically reviewed or when critical changes take place.

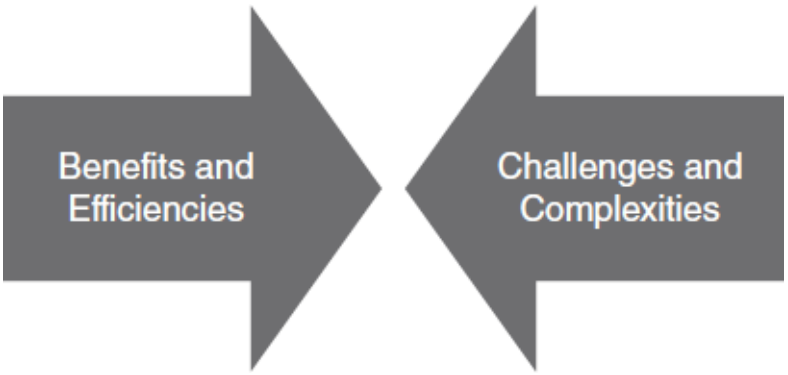
**Exam tip: Automated Failover is the best solution*

Exam Essential

- BCDR (RTO, RPO)
- Virtualization risk
    - Isolating VM within same Hypervisor
    - VM Sprawl
    - Inter VM attack
    - SDN attacks

Domain 4 - Cloud Application Security

Cloud Development typically include Integrated Development Environment (IDE), application Lifecycle management, and application security testing.



Benefits and Efficiencies tend to conflict with challenges and complexities.

Controls implemented at traditional datacenters should be exactly replicated to the cloud environment to make the cloud secure. Application at cloud is different from the conventional on-prem application.

The cloud application can be broken into three sub-components:

- Data
- Functions
- Processes

Components are broken so that portion that have sensitive data can be stored or processed in a specific location which that portion that has sensitive data can be stored or processed within a particular location that complies with enterprise policy.

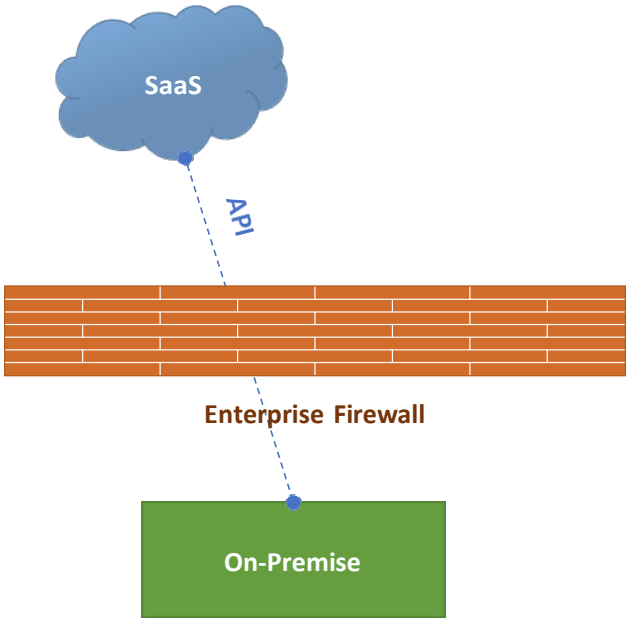
Determining Data Sensitivity and Importance

To determine sensitivity, ask for impact on the following questions

- Data is disclosed
- CCSP accessed the application
- Outsider manipulated process or function
- Process failed to provide expected result
- Data was changed (Integrity)
- Application was unavailable (availability)

Understanding API Formats

API uses tokens rather than traditional username and password.



Enterprise connects to CSP using APIs

1. **Representational State Transfer (REST):** A Software architecture style consisting of guidelines and best practices for creating scalable web services.

2. **Simple Object Access Protocol (SOAP)**: A protocol specification for exchanging structured information in the implementation of web services in a computer network.

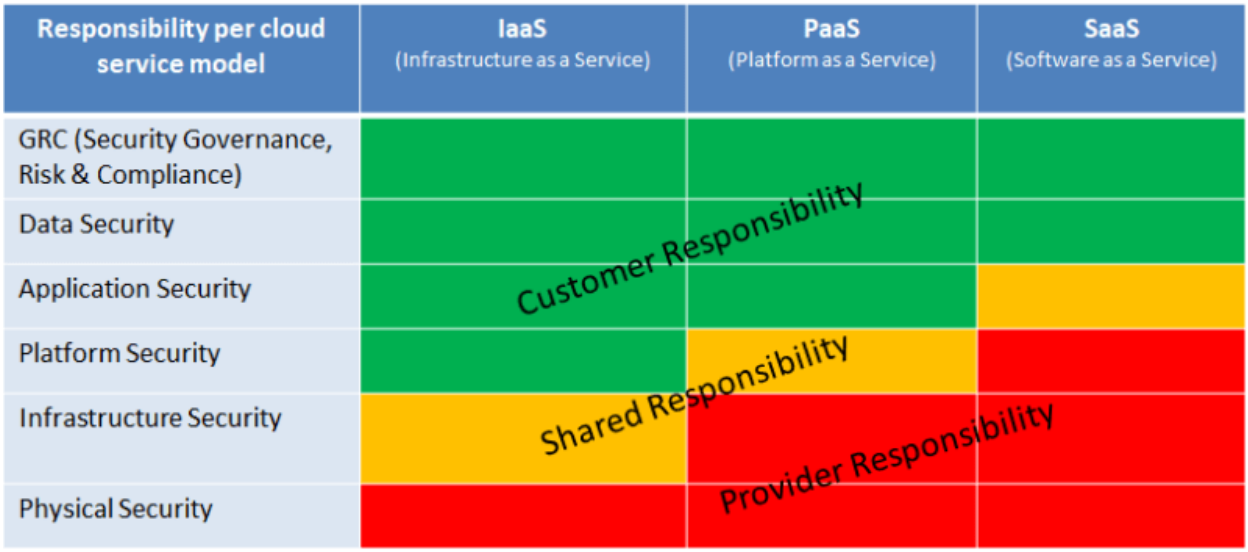
REST	SOAP (Heavy duty)
• HTTP • Flexible and Popular • Point to Point • Easy to use • No expensive tools • Supports multiple format JSON, YAML, XML • Fast	• Language, platform and transport independent (FTP, SMTP, HTTP) • Distributed Enterprise environments • Standardized, pre-build extensibility, Built-in error handling, Automation • Used where REST can't be used • Only supports XML

Common Pitfalls of Cloud Security Application Deployment:

- On-Prem does not always transfer (and vice-versa)
- Not all apps are "Cloud-Ready" – Legacy apps with high-security control
- Lack of training and awareness
- Lack of Documentation and Guidelines
- Complexities and Integration – CSP's API should be used to reduce complexity
- Overarching Challenges (Risk)
    - Multitenancy
    - Third-Party Admin

**Exam Tip: Forklifting an application is a process of migrating an entire application to cloud so it runs in a traditional environment with minimal code changes.*

**Exam Tip: ISO/IEC 12207: Standard for SDLC on Cloud.*



Responsibilities between CSP and Customers

Awareness of Encryption Dependencies

Applications running in the cloud should consider encryption:

- Data at Rest {at CSP}
- Data in Transit {CSP network or internet}
- Data Masking (or obfuscation) – to avoid data being viewed by CSP

Encryption provided by CSP, consider type, Algorithm, key management. Threat modelling should also be addressed.

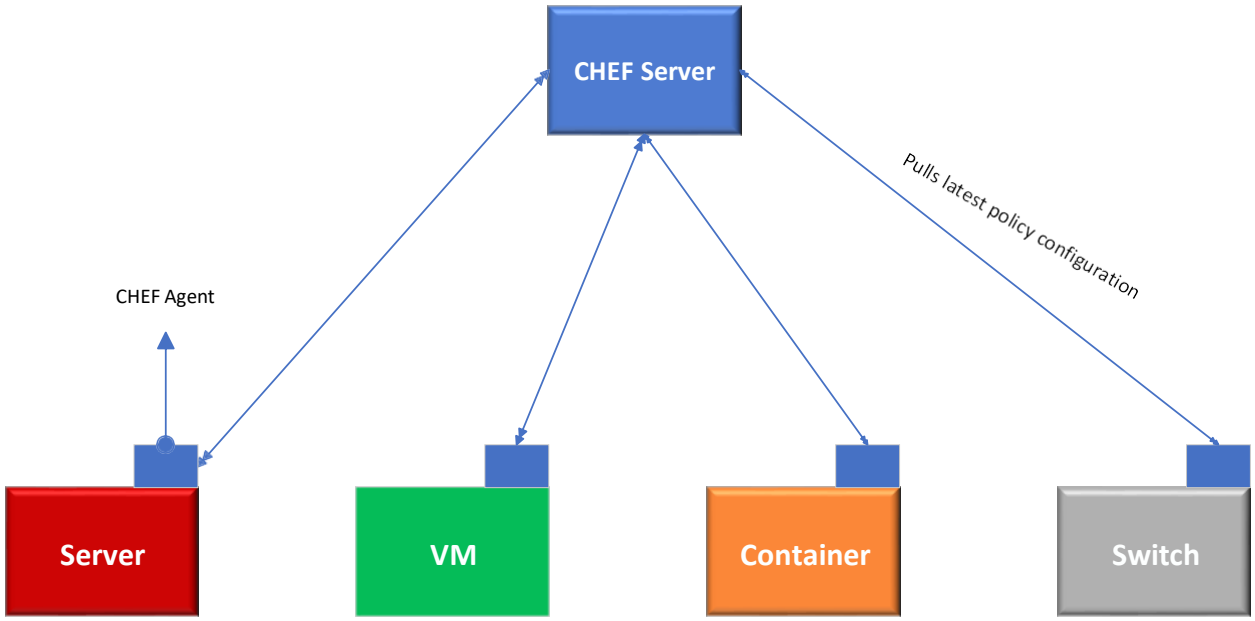
Understanding SDLC for Cloud Environment

- **Planning and Requirement Analysis:** Business and security requirements are determined. Main focus of the project.
    - QA and Risk identification is done
- **Defining:** Define and document product requirements and get it approved by the customer. Done through the Requirement specification document.
- **Designing:** Hardware and system requirements is gathered for overall system architecture. Threat modelling and secure design should be discussed.
- **Developing:** Work is divided into modules and coding is started. Longest phase. Code Review, Unit testing, and Static Analysis.
- **Testing:** Unit testing, integration testing, system testing, and UAT.

Secure Operation Phase

After SDLC, proper configuration management and versioning are essential to application security.

- **Puppet:** Configuration management system, which allows to define the state of IT Infra and enforces correct state.
- **Chef:** Automates the build, deploy, and manage infrastructure. Stores recipe as well as other configuration data.



Automated Policy deployment using CHEF

- Dynamic Analysis
- Vulnerability Assessment and Pentest
- Activity Monitoring
- Layer 7 Firewall – (WAF)

Disposal Phase

Application is decommissioned and keys used to encrypt data in the cloud are destroyed (a.k.a. crypto shredding).

Framework for improving critical Infrastructure Cyber Security

Core: Cyber Security activities are divided into 5 parts:

- Identity
- Protect
- Detect
- Respond
- Recover

Profile: To help the company align activities with the business requirement, risk tolerance and resources.

Implementation Tiers: To help organizations categorize where they are with their approach.

- Describe current cybersecurity posture
- Describe the target state for cybersecurity
- Identify the scope of improvement continuously
- Access progress towards the target state
- Communicate stakeholders about Risk

First Core (Framework) Identity (ID):

- Asset Management (IDAM)
- Risk Assessment (IDRA)

IDAM:

- IDAM-2: Software platforms and apps are inventoried
- IDAM-3: Org communication and Dataflow are mapped
- IDAM-5: Resources are prioritized based on classification, clarity, and business value.

IDRA:

- IDRA-1: Asset vulnerabilities are identified and documented
- IDRA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine the risk

Cloud Specific Risks:

- Security Controls should be baked in encryption
- Logging and Monitoring
- Application isolation

Top 9 cloud computing Threats

- **Data Breaches:** In multitenant cloud architecture, if proper controls are not there, a breach in one database can cause a breach in other tenants.

- **Data Loss:** Accidental deletion of data by CSP, fire or earthquake. The customer uploads encrypted data but loses the key.
- **Account hijacking:** If sessions are not adequately protected, it could lead to account hijacking.
- **Insecure APIs:** APIs should be authenticated, encrypted, and monitored.
- **Denial of Services:** If resources are not adequately prioritized and segregated, the victim cloud could starve the resources.
- **Malicious Insider:** Current or former employee contractor or other business partners
- **Abuse of Cloud Services:** Using cloud servers to stage DDOS attack, crack encryption keys, and serve Malware
- **Insufficient Due Diligence:** Lack of knowledge research about security and organization jumping to CSP
- **Shared technology issues:** Defense in Depth is recommended, isolation. A single vulnerability can lead to compromise across an entire provider's cloud.

Threat Modelling (Done at the design phase):

STRIDE:

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Escalation of privilege

Approved API

Benefits:

- Programmatic control and access
- Automation

- Integration with Third party tools

Consumption of External APIs should go through the same approval process as software being used in the organization. APIs should be secured. SSL (REST) or message level crypto access (SOAP). Authentication and API usage

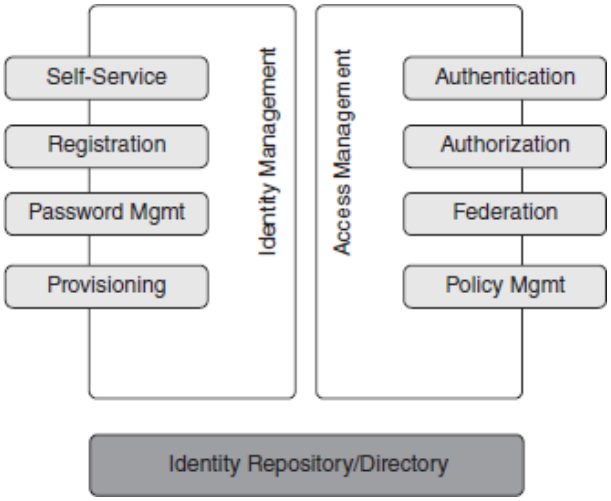
**ISO/IEC 27034-1 Secure Software development*

Software Supply Chain (API) Management

It's important to assess all codes and services for proper and secure functioning no matter where they are sourced.

Security Open Source Software: Largely and openly tested software is considered more secure.

Identity and Access Management (People, process, and system)



Identity and Access Management

Identity Management: Identifying individuals in as system and controlling their access to resources

Access Management: Managing an individual's access or a resource.

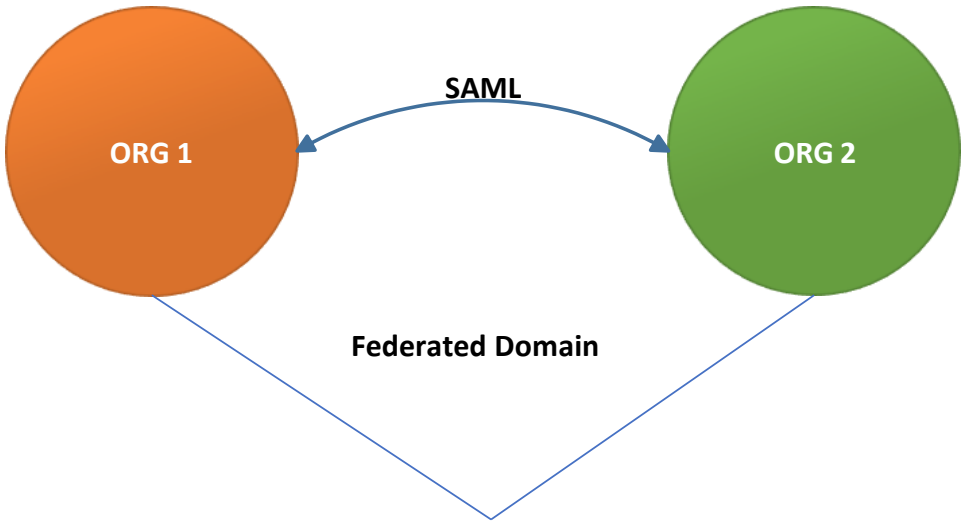
- Authentication
- Authorization
- Policy Management – Security and access policy based on business needs and risk appetites.
- Federation – Organizations exchange user's information
- Identity Repository – Directory services

Identity Repository and Directory Services: Provides administration of user accounts and their attributes.

Single point of Administration:

- X.500
- LDAP
- MS Active Directory
- Novell directory
- Meta Data replication and synchronization
- Directory as a Service.

Federated Identity Management



Identity Sharing

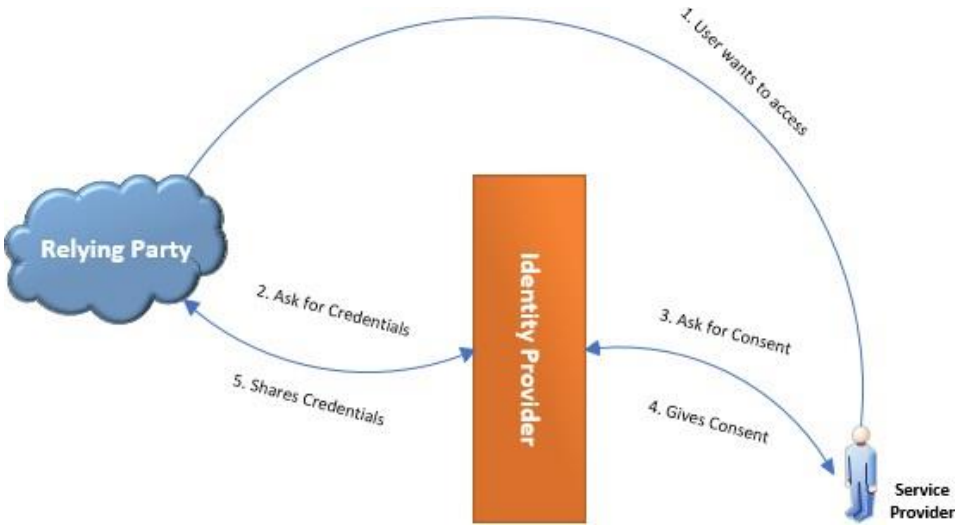
Federation Standard

SAML 2.0 is most commonly used. SAML 2.0 is XML based framework for communicating user authentication, entitlement, and attribute information.

Other Standards

- **WS-Federation:** Defines mechanisms to allow different security realms to federate, such that authorized access to resource at one realm can be provided to security principles, whose identities are managed in other domains.
- **Open ID Connect:** Interoperable authentication protocol based on OAuth 2.0
- **OAuth:** Used for authorization OAuth 2.0

Shibboleth Standard: User authenticates with their organization's credentials and the organization (Identity Provider) passes information to service providers.



Federated Identity Provider

In cloud, organization could become Identity Provider.

Federated SSO should not be confused with Reduced Sign-On (RSO) or password synchronization.

Users don't enter credentials to access resources in the same federated domain.

Multi-Factor Authentication: (*Combination of at least 2 types***)**

Type 1: Something you know

Type 2: Something you have

Type 3: Something you are

Step-up Authentication is an additional layer:

- Challenge questions
- Out of band authentication (SMS)
- Dynamic knowledge-based Authentication

Supplemental Security Devices

Add additional layers to defense in depth.

- Web Application Firewall (WAF):
  - Layer 7 Firewall
  - Cloud WAF is effective against DDOS
  - Analyze HTTP traffic

- Database Activity Monitoring (DAM):
  - Layer 7 monitoring device which understands SQL commands
  - Agent based DAM (ADAM) or NETWORK based DAM (NDAM)
  - It can detect and stop malicious commands from executing on the SQL server

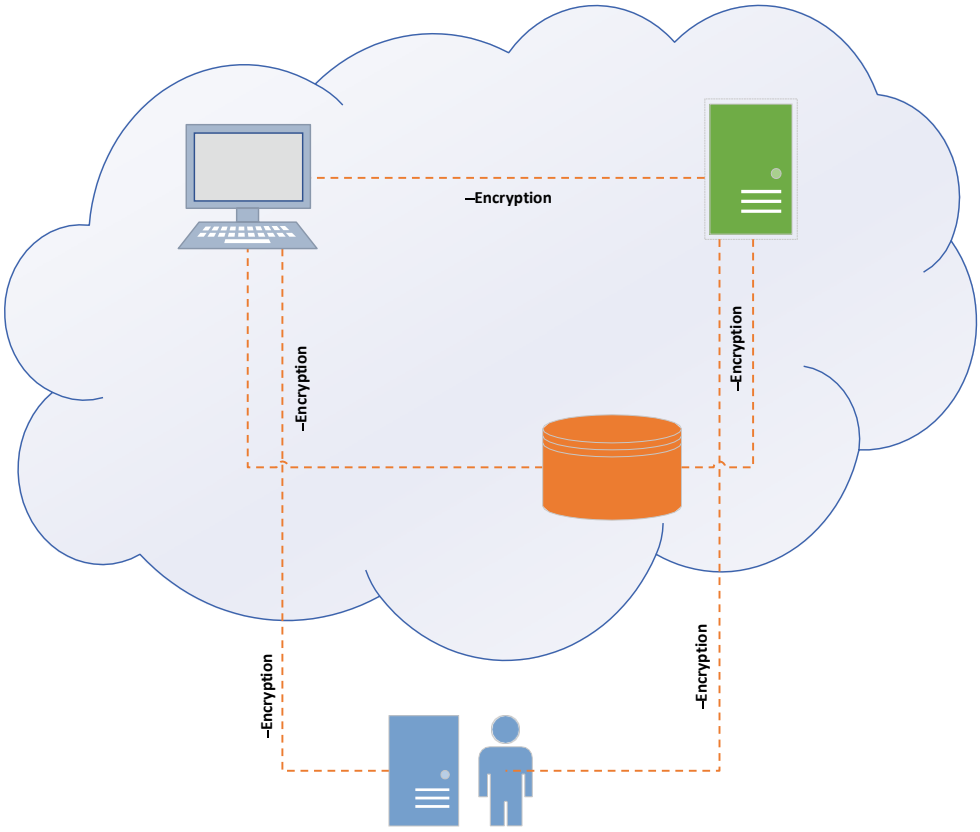
- XML:
  - XML Gateways enables the exposure of sensitive data as API
  - XML Gateways can either be hardware or software
  - It can implement control as DLP, AV, etc.

- Firewall: It can be distributed or configured across SaaS, PaaS or IaaS. It can be owned/operated by a provider or outsourced to Third party. Firewalls in the cloud need to be installed as software (Host-Based).

- API Gateway:
  - It filters API traffic. It can be installed as a proxy.
  - It can implement across controls, rate-limiting logging metrics and security filtering.

Cryptography:

- Transport layer security (TLS)
- SSL
- VPN (IPSeC)



Examples of Data at Rest

- **Whole instance encryption:** Method of encrypting all the data associated with the operation and use of the virtual machine. e.g. Data in transit from virtual machine and storage volume.
- **Volume Encryption:** Single volume of a drive is encrypted. Part of the drive is left unencrypted.
  {Full disk encryption is used to encrypt the entire drive}
- **File or Directory Encryption:** Method of encrypting a single file or directory on a drive.

Tokenization: It generates a token (a string of characters) and replaces sensitive data. Unauthorized users should see the token instead of real data. They are used in PCI DSS.

Data Masking: Keeps the format of the data but alters the content

Sand Boxing: It isolates and utilizes only intended components while separating the remaining components.

In cloud, untrusted codes are tested in sandbox.

Application Virtualization:

Creates a virtual environment for an application to run. Creates an encapsulation from the OS. Used for isolation.

Examples:

- Wine, allows MS apps to run on Linux platform
- MS App-V
- Xen App

**Exam tip: Main goal of app virtualization is to test application while protecting OS and other apps on a system.*

- **Software Assurance:** Ensuring software functions as intended with all the security controls in place.
- **Verification and Validation:** It should occur at each stage. To ensure consistency of the application.

Cloud-Based Functional Data: Data is not entirely equal. It should be included in the contract as which data is being handled by Third party and have any legal implications.

Cloud Secure Development Life Cycle: Vulnerability scan gives a point in time assurance of any application.

People, Processes, and Technology (PPT) gives a holistic view of software.

PPT who developed it and who will maintain

One SDLC	Another SDLC
1. Requirement 2. Design 3. Implementation 4. Verification 5. Release	1. Planning and Requirement 2. Defining 3. Designing 4. Developing 5. Testing 6. Maintenance

ISO / IEC 27034-1 (App Security)

Security of application should not only be considered as development but also regulatory and business context.

Service Oriented Architecture: Software with interoperable services

Organizational Normative Framework (ONF) – Bidirectional process

ONF	
Business Context	Specification
Regulatory Context	Roles
Technical Context	Processes
Application Security Control (ASC) Library	

- **Business Context:** Security policy, standards, and best practices adopted
- **Regulatory Context:** Standards, laws, and regulations that affect application security
- **Technical Context:** Includes required and available technologies that are applicable to App Sec
- **Specification:** Documents the organizational IT functional requirement and the solution that are appropriate to address these requirements.
- **Roles, Responsibilities and Qualification:** Factors related to IT applications.
- **Processes:** Relates to App Sec.
- **Application Security Control Library:** Contains approved control required to protect an application

**Exam tip: Bidirectional process is meant to create a continuous improvement loop*

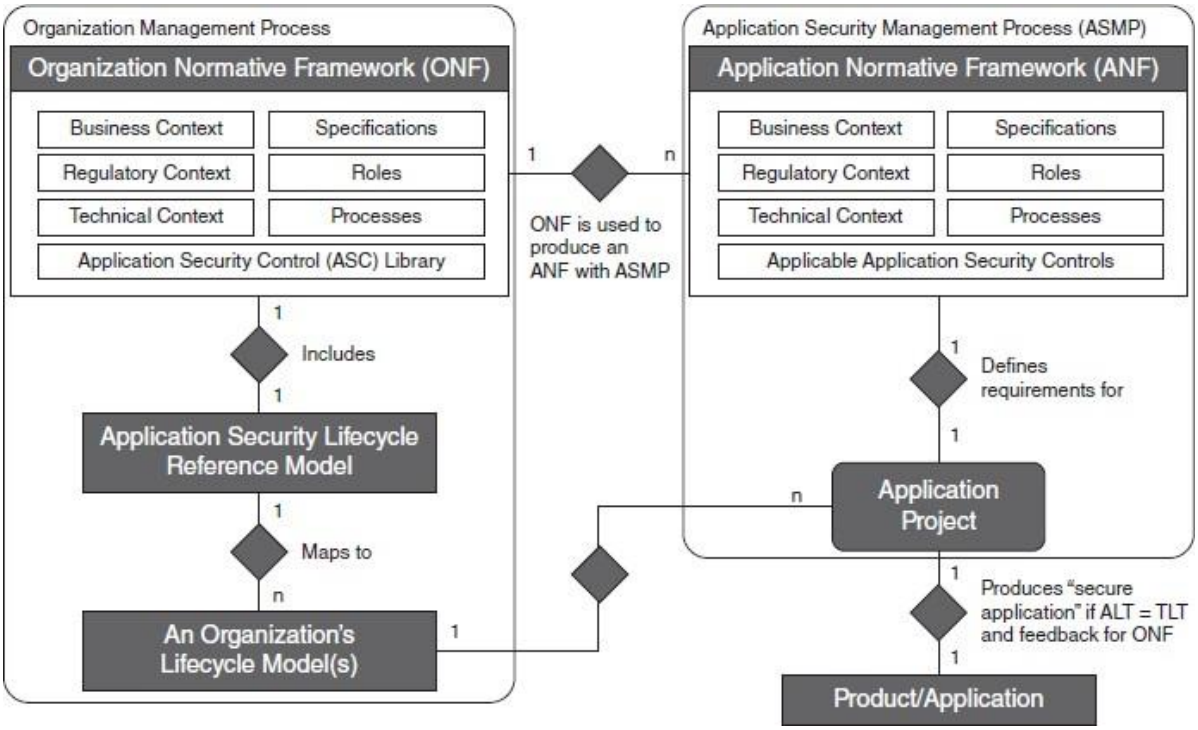
Application Normative Framework (ANF): Used in conjunction of ONF and is created for specific application.

**ONF to ANF has a one-to-many relationship.*

***ONF is used to create multiple ANFs.*

Application Security Management Process (ASMP): ISO / IEC 27034-1 defines ASMP to manage and maintain each ANF.

- Specifying the application requirements and environment
- Assessing application security risks
- Creating and maintaining the AMF
- Provisioning and operating the application
- Auditing the security of the application



ONF is used to produce an ANF with ASMP.

Application Security Testing

- **Static Application Security Testing (SAST):**
  - White box testing. Done without executing the application.
  - Determines coding errors. Early development life cycle.
  - Useful for XSS, SQL Injection, Backdoors.

- **Dynamic Application Security Testing (DAST):**
  - Black box testing. Done at the runtime.
  - Useful to test exposed HTTP and HTML Interfaces.

- **Runtime Application Self Protection (RASP):**
  - Considered to focus on application that possesses self-protection capabilities. Prevents attacks by self-protecting without human intervention.

- **Interactive Application Security Testing (IAST)**
  - Uses sensors or agents that run withing application to identify vulnerabilities based on performance and workings.
  - Potential issues are identified earlier and can be integrated with CI/CD pipeline

- **Vulnerability Assessment and Penetration Testing:** VA looks for vulnerabilities and PT exploit those vulnerabilities.

**Exam tip: SaaS providers don't allow clients to execute Pentest for their environment.*

- **Source Code Reviews:** Informal and formal review of code is done.

- **OWASP Recommendation:** 9 types of active security testing:
    - Identity management testing
    - Authentication testing
    - Authorization testing
    - Session Management testing
    - Input validation testing
    - Testing for error handling
    - Testing for weak cryptography
    - Business logic testing
    - Client-side testing

DevOps Security

Fundamental principle of DevOps is to combine the efforts of development, Quality Assurance and IT Operations. This is done to accelerate the process development, integration and delivery of projects from build to production. This is often done with Continuous Integration and Continuous Delivery (aka CI/CD). However, combining these processes violates one of the core principles of security i.e., Segregation of duties (SoD). Idea of DevOps Security or DevSecOps is to integrate the security piece in the DevOps. This is often achieved by the following approaches.

- Educating developers to write secure codes to ensure the applications are not only functionally mature but also has minimum security flaws.
- Introducing the concepts of security champions to cascade the security knowledge among developers and act as a contact point for any security recommendation.
- Introducing the concept of "Shift-Left" were most of the testing is done at the development phase.
- Establishing Software Composition Analysis to make sure open-source configurations or components like "log4j" are evaluated before getting introduced in the environment.

Exam Essential

- API - REST vs. SOAP (use cases, drawback)
- Using unapproved API enhances productivity
- OWASP - SQL injection, XSS, CSRF
- SDLC phases
- How to verify secure Software

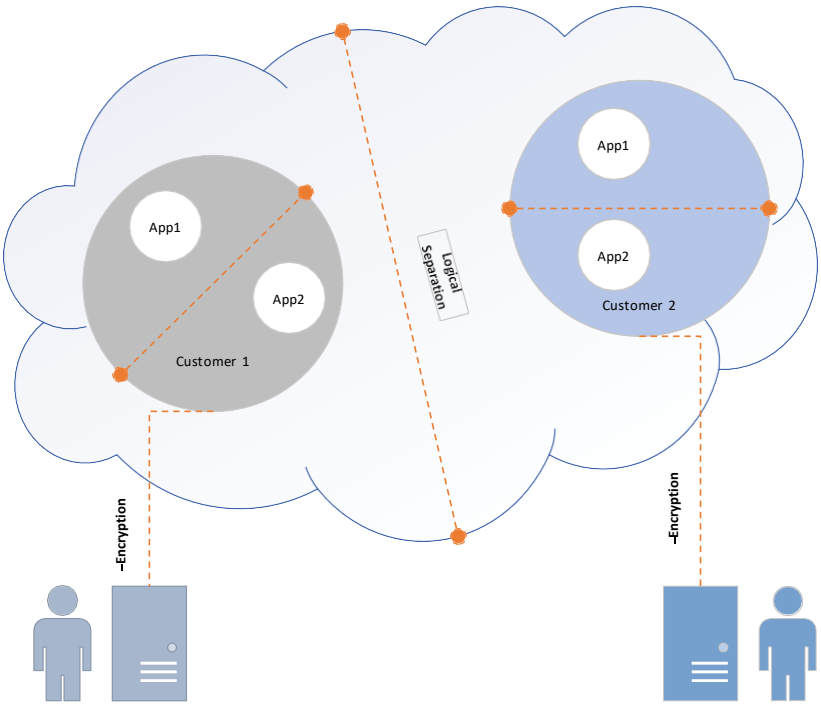
Domain 5 – Cloud Security Operations

Factors that affect Data Center Design:

1. Location (Legal and Regulatory (jurisdiction))
2. Contingency, failover, Redundancy
3. Compliance Requirement
4. Operation Standard: ISO27001:2013, ITIL, ITSM
5. Physical and Environmental Design

Logical Design

- Multitenancy

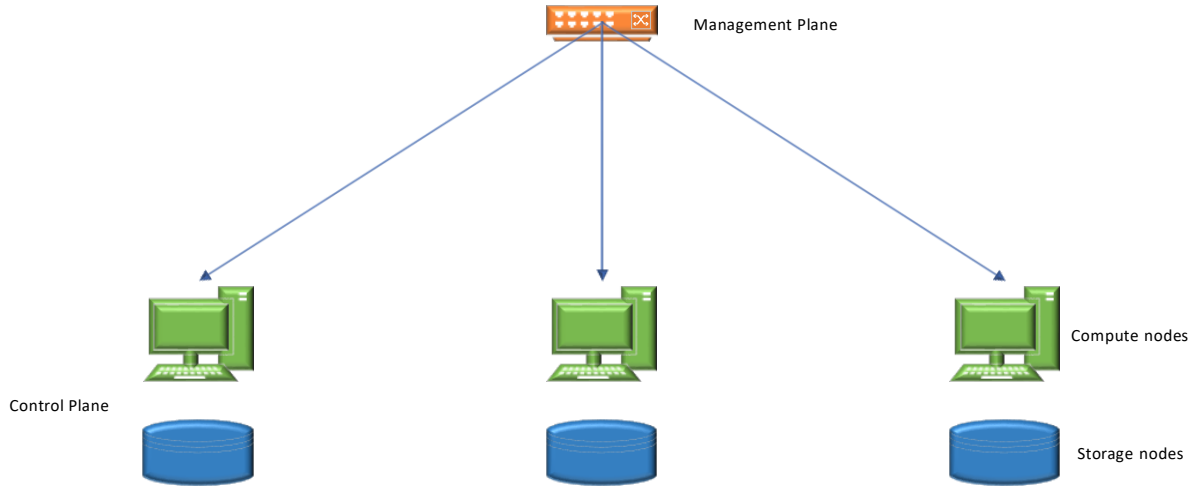


- Cloud Management Plane (CMP):
  - Configuration Management
  - Service Lifecycle Management
  - SLA Management
  - Logging, Monitoring, and Auditing
  - Security Services and Infrastructure Management

- Virtualization Technology:
  - Communication access, API access
  - Secure communication within and across the Management plane
  - Secure Storage (encryption, key management, and partitioning)
  - BCDR, Failover, and Replication

- Other Design Consideration:
  - Separation of Duties
  - Monitor network traffic (to and fro on Management Plane)
  - Automation and use of API
  - IAM Solution
  - SDN

- Logical Design Level:



- Service Model:
  - IaaS (use of Hypervisor)
  - PaaS (logical design on Platform and Database)
  - SaaS (control in applications)

Physical Design: Physical Design should shape the environmental design of the Data Center

Building or Buying?

- Data Center tier certification
- Physical security level
- Multitenant or dedicated

**Exam tip: When using Standard DC, physical separation of servers is necessary.*

Data Centers Design Standards

- Building Industry Consulting Service International INC (BICSI):
  - Cabling and Design installation
- The International Data Center Authority (IDCA):
  - Data center location, facility structure, and infra-structure and application
- National Fire Protection Association (NFPA):
  - Requirement for temperature, emergency

Data Center Site Infrastructure Tier Standard Topology: Baseline for Data Center design

Lowest

↓

Tier 1: Basic Data Center Site infrastructure

Tier 2: Redundant site infrastructure capacity components

Tier 3: Concurrently Maintainable site infrastructure (*suitable for financial institutes*)

Tier 4: Fault-tolerant site infrastructure (*suitable for health care providers*)

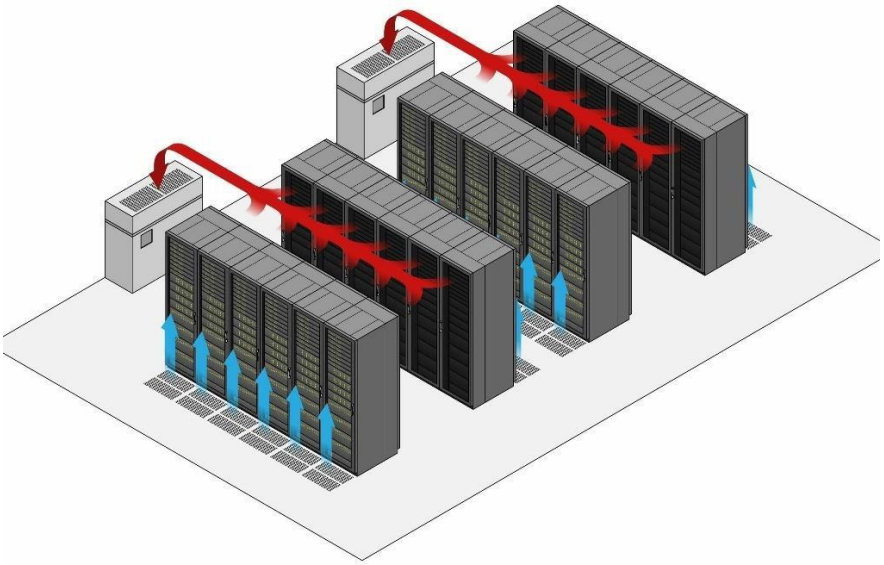
↑

Highest

**Exam tip: Network connectivity should be from multiple vendors*

Temperature: 64.4° (18°C) – 80.6°F (27°C)

Moisture: 40% - 60%



Air Management in Datacenter and Aisle containment

Secure Configurations of Hardware Specific Requirement

**Actual settings of the hardware depending on OS and virtualization*

Best Practices for Servers

- Secure build
- Secure initial configuration

Common best practices

- Host hardening
- Host Patching
- Host Lockdown
    - Block non-root access
    - Secure Connection
    - Host-based firewall
    - RBAC
- Secure on-going configuration maintenance
    - Patch Management, VA/PT

Best Practices for Storage Controller

iSCSI, FCoE, etc.

These should be protected as per the guidelines given by the vendor and additional security.

iSCSI is a protocol that uses TCP to transport SCSI (*Small Computer System Interface*) commands, enabling the use of existing TCP/IP network infrastructure as SAN.

Initiator: The consumer of storage.

Target: Ports on the storage system that deliver storage volumes (target devices).

*iSCSI should be considered as LAN and not WAN due to latency and security issues

Oversubscription: No. of users connected to the system are more than the system supports.

- Dedicated LAN for iSCSI
- Not to share storage network

iSCSI implementation consideration:

- **Private Network:** As iSCSI traffic is sent unencrypted, a private network is needed
- **Encryption:** IPSeC, IKE, VPN
- **Authentication:**
    - Kerberos
    - Secure Remote Password (SRP): Secure Password-based authentication
    - Simple Public-Key Mechanism (SPKM): Provides
        - Authentication

- Key establishment
- Data integrity
- Data confidentiality using PKI
- Challenge Handshake Authentication Protocol

**Physical switch: If cable goes down, a particular switch will be down.*

**Virtual switch: In this, the entire VM will be down*

Virtual Switch: Connecting Physical NIC to virtual NIC in VM

- Redundancy
- Segmentation
- Security

**Exam tip: Redundancy can also be achieved through the use of Port Channeling*

Network Isolation:

- Each management network should have virtual and physical isolation
- Live movement of VM from one host to another is done in exact text (MiTM)
- Lockdown virtual switch

Physical security stacks (IDS, IPS) may not prevent VMs threats.

- For better virtual, network security strategy, use security applications designed specifically for virtual infrastructure
- For storage iSCSI or NFS, use proper authentication. **iSCSI, bidirectional CHAP is best.*

Isolation and Configuration of virtualization Management Tools for Host

Protect Management Plane (tools):

- Isolation
- Continuous security onitoring
- Vulnerability test for management tools
- RBAC
- Logging and Monitoring

Leading Practices:

- Defense in Depth
- Access Control
- Auditing and Monitoring – logging and monitoring

- Maintenance – patch

Running a Physical Infrastructure for a Cloud Environment: Important consideration when sharing resources

- Legal
- Compatibility
- Control *Who handles the Key Management for encrypted data?*
- Log data
- PCI DSS access
- Upgrades and Changes
- Failover Technology
- Compliance
- Regulations: SOX, GLBA, HIPAA, PCI-DSS. Data owner is responsible for compliance.
- Outsourcing: Losing control over data
- Placement of security
- Virtualization
- Virtual Machine – Virtual Machine is vulnerable as they move between the public and private cloud.

**OS and Application files:* *Responsibility of Patching is with subscriber instead of CSP.*

**Data Fluidity:* *Data is fluid in Cloud computing (on-Prem to off-Prem).*

**Exam tip: In the cloud computing world, CSP is in charge of customer data security and privacy*

Configuring Access Control and Secure Kernel-based Virtual Machine

Access (Physical and Logical) should be given on a need to know basis. Access to hosts should be through secure kernel-based VM **(KVM)** (*Converts Unix (OS) to Type1 Hypervisor, inbuilt part of Linux)*

Design for Secure KVM:

- Isolated data channels
- Tamper warning labels on each side of KVM
- Housing intrusion detection
- Fixed Firmware
- Tamper Proof Circuit Board
- Safe Buffer design
- Selective USB design
- Push-button control – Physical access needs to switch between computer

**Exam tip: Access restriction to the VM console is also important. (RBAC and logging / monitoring)*

Securing the Network Configuration:

- TLS and IPSeC – Confidentiality
- DNSSEC
- VLAN

Network Isolation: It is a critical design concept for a secure network configuration in cloud environment.

**Management plane should always be isolated.*

Achieved through VLAN:

- All network should be audited
- Access Restriction (RBAC)
- Strong authentication

Protecting VLAN's: VLAN: Putting 2 or more systems on the same LAN in a way that only those 2 systems can communicate with each other.

Transport Layer Security: Uses X.509 certificates to authenticate to connection and exchange symmetrical key for encryption.

TLS made up of 2 layers:

- **Record Protocol:** Connection security ensure connection is secure and reliable. Used to encapsulate high-level protocol.
- **Handshake Protocol:** Used for authentication between client and server and to negotiate an encryption algorithm and keys before sending / receiving data.

Domain Name System: IP address to Domain names

DNSSEC: Protection against DNS poisoning

Threats to DNS infrastructure:

- Foot Printing: Process where attacker obtain DNS Zone data
- DOS Attack
- Data Modification
- Redirection
- Spoofing

IPsec: Uses mutual authentication at the time of session establishment. Provides Confidentiality, Authenticity, Integrity, and Non-repudiation.

Challenges with IPsec

- Configuration Management: Components in cloud may not be IPsec compatible
- Performance: There is a slight degrade in performance

Identify and understand Server Threats

**Risk assessment should be performed better to understand the security posture of servers and systems.*

Guidelines:

1. Use an Asset Management System
2. Use system baselines to enforce configuration management
3. Consider automation technologies for checking system baselines
4. Develop and use a robust change management
5. Use vendor specified configuration guidance and best practice

Using Stand-alone Host: Think about all possibilities in an organization that wants to move their existing application to Cloud (*an example of ABC Corp. moving CRM application*).

Using Clustered Host

A clustered host is an arrangement to put multiple systems (or VMs) logically and physically connected to each other to offer fault tolerance. In case one of the nodes in the cluster fails, the failover happens to another available node. For the end-user, it appears as a single system.

- **Resource Sharing:**
  - **Reservation:** Min. guarantee of the resource available
  - **Limit:** Max. amount of resource available
  - **Share Provision:** Remaining resources will be shared based on the priority (Resource Contention)

- **Distributed Resource Scheduling / Compute Resource Scheduling (DRS/CRS):** All virtualization vendor uses DRS for:
  - High availability (HA)
  - Balance workloads
  - Scale and Manage Computer Resources

**Exam tip: Load Balancing is achieved through movement of VM between hosts in Cluster. This movement is controlled through affinity (Grouping) and Anti Affinity (separation).*

Accounting for Dynamic Operation:

***Elasticity is defined as degree to which a system can automatically adapt to workload changes by provisioning and de-provisioning resources.

Using Storage Clusters: Use of 2 or more storage servers working together to increase performance, capacity, or reliability.

Clustered Storage Architecture:

- **Tightly Coupled:** Both nodes work together to increase performance
- **Loosely Coupled:** Performance and capacity limit

Goals of Cluster Storage:

- Meet SLA
- Separate customer data in multitenant hosting
- Protect CIA of data

High Availability (HA) in Cloud:

- Redundant Architecture
- Multiple vendors for the same service

**OS baselining is very important.*

Performing Patch Management:

Identify → Acquire → Installing → Verifying

Areas of Automation (Patch Management):

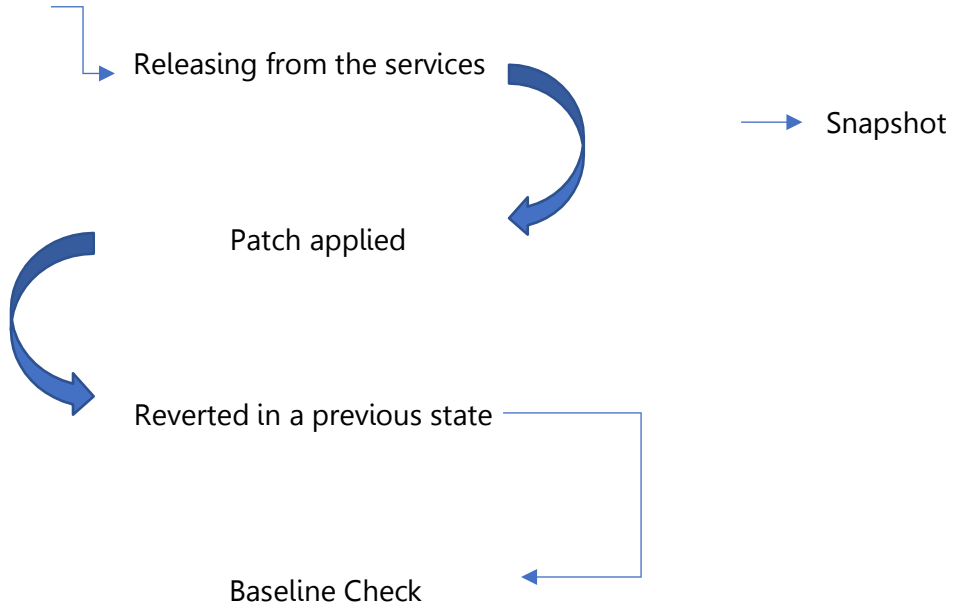
- Security Patch applicability
- Change record creation, approval, and implementation
- Creation of tracking records
- Verification of the implementation of patches
- Documentation

Challenges:

- Lack of service standardization
- It's a collaboration of multiple tools and processes
- Thorough testing of patch is required in case of automatic implementation
- VM running in multiple time zones

Multiple Time Zones: The same patch needs to be implemented to multiple VMs in a different time zone

VM Suspension and Snapshot:



Performance Monitoring:

- **Network:** Monitoring dropped packets
- **Disk:** Full disk (Slow read / Write Ops)
- **Memory:** Excessive memory usage
- **CPU:** Excessive CPU utilization

Outsourcing Monitoring: Due care and due diligence before outsourcing

- HR Check
- Define SLA
- Trial service before signing contract

Hardware Monitoring: Monitor Physical Infrastructure

Redundant System Architecture: Make your infrastructure redundant and resilient

Monitoring Functions: Monitoring to ensure any system failure is identified beforehand

Backing up and Restoring the host Configuration:

- **Control:** Who and what is allowed to access consumer data and programs and ability to perform an action
- **Visibility:** Ability to monitor consumer data (who is accessing what)

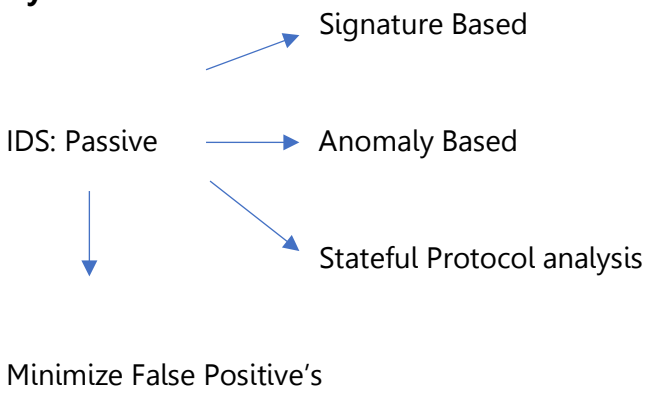
Implementing network Security Controls:

- Defense in Depth

Firewall:

- Host-Based: Effective for small infrastructure in Private Cloud

Layered Security



Network IDS (NIDS): Works in Promiscuous mode

Host IDS (HIDS): Takes snapshot of existing file systems and matches to the previous snapshot

Intrusion Prevention System: Can also drop malicious traffic. IPS can respond in the following ways:

- Reconfigure the security controls
- Removes malicious context from the packet

Virtual Machine Introspection (VMI)

Allows for agents less retrieval of the guest OS state (Running Process, active network connection).

VMI can do external monitoring for IDS and IPS and can be used for malware analysis, memory forensics, and process monitoring.

Honeypot: Isolated system to lure attackers.

IaaS – No access to logs

PaaS and SaaS – May have access to logs

**Exam tip: A log should be preserved, classified, and protected. Logs should be captured based on NTP.*

Developing a Management Plan:

Maintenance: During the maintenance window, CSP should ensure they can meet the SLA. Use automated tools to send out the notification. The host is placed on maintenance mode before starting any work that requires system downtime.

Orchestration: , The goal of cloud orchestration, is to automate the configuration, coordination, and management of software and its interaction.

Building Logical Infrastructure for Cloud Environment

- **Logical Design:** Part of the Design phase in SDLC
  - It lacks technology detail and standards
  - It communicates with abstract concepts (network, routers, system)

- **Physical Design:** To show the hardware used to deliver the system
  - Created from logical design
  - Expands element from logical design

Infrastructure as Code (IaC) Strategy: IaC is about configuring the infrastructure through codes rather than doing manually. Configuration files are created which contain the infrastructure specifications making it easy to edit and distribute the configuration. This also aids the configuration management process of the organization and reduce the risk of undocumented configuration changes.

Networking Models

- **Traditional:** Physical switch at top layer and logical separation at hypervisor level
- **Converged Networking:** Optimized for cloud deployments which are capable of carrying a combination of data, voice, and video traffic across a single network

Running a logical infrastructure for Cloud environment: Secure configuration to ensure isolating customer data to prevent DOS attacks.

Building secure NETWORK configuration:

- VLAN
- TLS
- DNS (DNSSEC)
- IPSeC

OS Hardening via Application Baseline:

- Capturing a Baseline: Look for the bare minimum-security requirement
- Baseline configuration by Platform
- Windows: Windows Server Update Service (WSUS), MS Deployment Toolkit (MDT), SCCM

- Linux: Linux distribution
- VMware: VMware Update Manager (VUM)

Availability of Guest OS:

- High availability (HA): Should be a part of the BCDR environment
- Fault Tolerance

Managing the Logical Infrastructure for Cloud Environment

- Access control for Remote Access
  - Change credential after vendor logged in
  - Use SSL/TLS

- Use of Cloud to reduce attack surface: Access made through the cloud ensures the internal network is not exposed. It acts as a proxy that mediates an untrusted network to a trusted (or internal) network.

  Benefits of Remote Access:

  - Secure access without exposing credentials
  - Accountability
  - Session control over who can access
  - Real-time monitoring
  - Secure isolation between client and target system

- OS Baseline Compliance, Monitoring, and Remediation: Tools to monitor OS baselining (VUM and WSUS)

- Backing up and restoring the Guest OS Configuration

Implementation of network Security Controls:

- Log capture and Analysis (logs needs to be protected)
- Management Plan implementation through Management Plane (Customer is responsible for security architecture and Resiliency)
- Ensuring Compliance with Regulations and Control (Refer Cloud Security Alliance Cloud Control Matrix)

Using an ITSM Solution: Drive and coordinate communication may be useful

- Portfolio Management
- Demand Management
- Financial Management

Shadow IT: Defined as money spent on technology to acquire services without the IT department's dollar or knowledge (*Expense of no use*)

Operations Management

- Information Security Management
- Configuration Management
  - Change Management.
  - Availability Management

- Change Management: Primary goal within the project management context is to create and implement a series of process that allow changes to the scope of a project to be formally introduced and approved

Request → Review → Approve → Implement → Document

- Incident Management:
  Identify → Analysis → Correct → Prevents future occurrence

  3 purpose and 5 objectives

**Exam tip: Incident Management plan should be routinely tested and updated based on lessons learned from real and practice events.*

Incident Classification: Based on its severity

The Impact / Urgency / Priority matrix

Urgency →

Impact ↑

	High	Med	Low
High	1	2	3
Med	2	3	4
Low	3	4	5

- Problem Management**:** Objective is to minimize the impact of problems on the organization.
  - A problem is the unknown cause of one or more incidents, often identified as a result of multiple similar results.
  - A known error is identified the root cause of a problem.
  - A workaround is a temporary way of overcoming technical difficulties.

- Release and Deployment Management:
  Plan → Schedule → Control the movement of release from test and live environments.

  The primary goal is to ensure that the integrity of live environment is protected. New software releases should be done as per the configuration management plan. Release management is especially important for SaaS and PaaS.

- Service Level Management: Aims to negotiate agreements with various parties and to design services under agreed upon service level target.
  - SLA
  - Operation Level Agreement (OLA)
  - Underpinning contracts (UC)

- Availability Management: IT systems should be available for the agreed-upon available targets.
- Capacity Management: It's a critical function. The system capacity must be monitored and thresholds must be set to prevent systems from reading an over the capacity situation.
- Business Continuity Management: ISO 22301:2012. Plan should be tested at regular intervals.
- Continual Service Improvement Management: Continuous improvement using a formal process (ITIL can be used as a tool).

The Risk Management Overview:

Four components

- **F**raming Risk
- **A**ssessing Risk
- **R**esponding to Risk
- **M**onitoring Risk

FARM

Framing: Allows the organization to articulate the risks that it needs to managed.

Risk Assessment:

- Identify Assets
- Vulnerability
- Threats
- Likelihood
- Impact

(a) **Qualitative:** Subjective

(b) **Quantitative:** Figures $ (Time and Effort required)

SLE * ARO = ALE
SLE = AV * EF
Risk = Likelihood * Impact

Critical Aspects of Risk Assessment:

- Risk of service failure and associated impact
- Insider threat (Admin accusing customer data in Cloud)
- Risk of compromised customer
- DOS
- Supply chain Risk to the CSP

**Exam tip: Risk Assessment should be conducted annually*

Risk Response:

- Acceptance
- Avoidance
- Transferred
- Mitigated

Reduce Risk: Leftover Risk

Risk Assignment: Who owns the Risk

Countermeasure Selection: Following points should be considered before choosing a countermeasure.

- Accountability (can be held responsible)
- Auditability (can be tested)
- Trusted source (source is known)
- Independence (self-determining)
- Consistent application
- Cost
- Case of use and reliability etc.

Risk Monitoring: Keeping track of identified risks

- Determine ongoing effectiveness
- Identify risk impacting changes
- Verify that planned risk responses are implemented

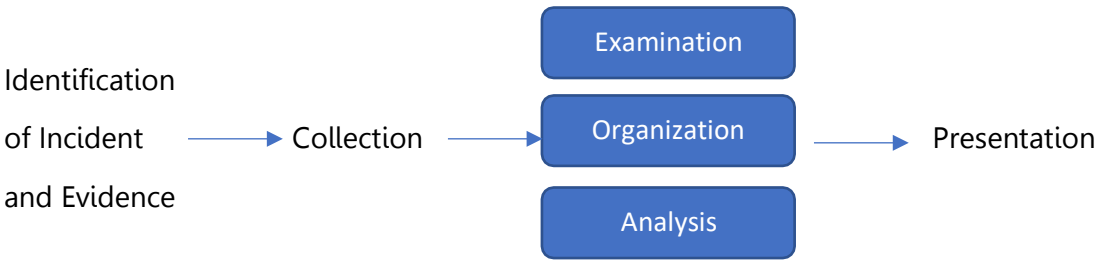
Understanding the collection and Preservation of Digital Evidence

- **Cloud Forensic Challenges:**
  - Control over data
  - Multitenancy
  - Data volatility (chain of custody is difficult)
  - Evidence acquisition

- **Data access within Service Model:** Access to data will be different for IaaS, PaaS, and SaaS.

- **Forensic Readiness:** Many incidents can be handled more efficiently and effectively if forensic consideration has been incorporated into the information system lifecycle.

- **Proper Methodology for Forensic Collection of Data:**



- **Collection:** Identifying, labeling, recording, and acquiring data from a possible source of relevant data
- **Examination:** Processing collected data
- **Analysis:** Analyzing the results of the examination
- **Reporting:** Reporting the results of the analysis

Data Acquisition and Collection:

- Develop a plan to acquire the data
  - Likely value
  - Volatility
  - Amount of effort required
- Acquire the data
- Verify the integrity of data

Challenges in Collecting Evidence:

- Collecting data from Host OS
- Collecting data from Guest OS
- Collecting Metadata

Examining the Data

- Bypassing OS to access data
- Using test and pattern searches to identify data
- Using a tool to determine the content of data
- Using knowledge of data file type to identify files
- Using any database containing information about known files to include or exclude

Analyzing the Data: Use Security Information and Event Management (SIEM)

Reporting the Findings:

- **Alternative Explanations:** The cause of an event can be more than one. Consider both explanations.
- **Audience Consideration:** What to show to whom
- **Actionable Information:** What can be done with the information collected

The Chain of Custody: You must take care when gathering, handling, transporting, analyzing, reporting, and managing evidence.

Evidence Management: Have policies and procedures for evidence management. (from collection to trial)

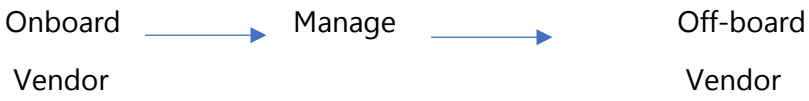
**Exam tip: Don't collect evidence outside of the scope*

Managing Communication with Relevant Parties

Five Ws & One H

- Who is the target of communication?
- What is communication designed to achieve?
- When is the communication best delivered?
- Where is the communication pathway managed from?
- Why is communication needed?
- How is the communication being transmitted?

Communication with Vendors and Partners



Communicating with Customers: Customers (external and internal) should be identified.

Communicating with Regulators: Early communication with regulators is vital while setting cloud. Infrastructure should be compliant with all regulations.

Communicating with Other Stakeholders: Additional parties should be identified and communicated periodically.

Exam Essentials

- ITIL
- Problem Management and Incident Management
- Change management and patch management
- Configuration and patch management
- Vendor Management
- Forensic Investigation (IaaS, PaaS and SaaS)
- SLA contracts, Risk Management
- Planning Data Centre and cooling system

Domain 6 – Legal, Risk and Compliance

❖ **To deal with legal issue, the first step is to contact the right professional.**

Legislative Concepts:

- International Law:
  - International Convention
  - International Customs
  - General principles of law
  - Judicial decisions
- State Laws: The law of each state (50 states in US)
- Copyright and Piracy law
- Enforceable Government Request: Order that is capable of being performed based on govt's order
- Intellectual Property right: Patents, trademarks
- Privacy law
- The doctrine of Proper law: When a conflict of laws occurs (*jurisdiction*)
- Criminal law
- Tort law or Civil law
- Restatement (second) conflict of laws: Development in the common law that informs judges and the legal world of updates in the area.

GDPR:

- Lawfulness
- Transparency
- Purpose
- Data optimization
- Accuracy
- Storage limit
- Security
- Accountability

Frameworks and Guideline relevant to Cloud Computing:

- **ISO/IEC 27017:2015:** Security Techniques
- **Organization for Economic Cooperation and Development:**
    - Privacy and Security Guidelines (OECD)
    - National Privacy Strategies
    - Privacy Management Programs
    - Data Security Breach Notification
- **Asia Pacific Economic Cooperation Privacy Framework (APEC):** Regional Standard to address Privacy
    - Privacy as an international issue
    - Electronic Trading environments and the effects of cross border data flows

**Exam tip: Goal is to promote a consistent approach to information privacy protection to ensure the free flow of information within the region.*

- **EU Data Protection Directive:** Protection of data collected for EU citizens.
- **General Data Protection Regulation:** Supersede the EU Data Protection Directive
    - **Directive**: Allows each country to create own law and comply with it
    - **Regulation:** Mandates all countries to comply with the regulation itself
- **EU-Privacy Directive:** Processing of personal data and protection of privacy in the electroniccommunication sector.

**Exam tip: Accountability is with customer while sourcing infrastructure from CSP, ensuring complying with different laws and regulation is also a customer's responsibility.*

e-Discovery: *(can be done online or off-line)*

Process in which electronic data is sought, located, secured, and searched with the extent of using it as evidence in a civil or criminal case.

**Exam tip: In cloud, e-discovery is always done online.*

e-Discovery Challenges:

Who controls the data? CSP owns a lot of data in cloud environment.

Considerations and Responsibility of e-Discovery:

Relation with CSP is very important. We need to understand as where's the actual storage of data within the cloud. Data held in multiple jurisdictions would be a challenge (Different laws in different regions).

Reducing Risk:

Contract with CSP should include "in case of an event, customer should have full control of data or if the subpoena is issued."

This should be included in the Business Continuity and incidence response plan.

Conducting e-Discovery Integration:

- **SaaS-based e-discovery:** Tools used for e-discovery – Cloud-based tools
- **Hosted e-discovery (CSP):** Provider does e-discovery
- **Third party e-discovery:** Outsource in case no pre-arrangements

Cloud Forensics and ISO/IEC 27050-1:

Protecting Personal Information in the Cloud

As customer's data can be placed anywhere, it becomes challenging for the customers to ensure data security requirements are met.

Difference between Contractual and Regulated PII:

- **Contractual PII:** When an organization shares PII to either CSP or outsource (call centers), they should include in the contract about the adherence of compliance in protecting the PII.
- **Regulated PII:** Must adhere to the law and statutory requirements.

Mandatory Breach Reporting: Notify and inform individuals of any security breach involving PII.

Contractual Components

- **Scope of Processing:** Purpose of the data being processed – Why?
- **Use of Subcontractors:** Where the processing of data will happen? Any subcontractors involved?
- **Deletion of Data:** Data should be deleted according to the organization's data retention and purging policy.
- **Appropriate or required data security controls:** When data is processed by an external entity, the same level (or higher) of controls should be implemented as on-prem (Defense in-depth and encryption {DIM and DAR}).
- **Location of Data:** Knowledge about the location of data being processed by contractors and subcontractors is important.
- **Return or reinstitution of Data:** Once the contract is terminated, all data should be returned to customer in a timely manner.
- **Right to audit subcontractors:** Right to audit clause should be included in the contract.

Contract Specific Legislation and Regulations related to PII, Data Privacy, and Data Protection

- **European Union:** Personal data outside EU is prohibited until and unless proper control is there.

  Directive 95/46 EC – European Convention of Human Rights (ECHR)

  EUGDPR – Replacement of EU directive

- **UK and Ireland:** Obtain consent before the transfer of any data.

  Consider the following:

  - **Security of data –** lies with the data controller
  - **Location of data**
  - **Requirement for a contract between CSP and Sub processors**

- **Argentina:** Personal Data Protection Act 2000. Data transfer between EU and Argentina can be done freely, as PDPA consists EU rules.

- **United States:** US doesn't have its own data privacy act.

Safe Harbor: US Department of Commerce and EU

- Notice
- Choice
- Transfer to Third parties
- Access
- Security
- Data Integrity
- Enforcement

**Exam tip: If not Safe Harbor, Standard Clauses can be implemented in the form of contract.*

- **HIPAA:** US Act. Protection of Health Information
- **GLBA:** Federal Law for US Banks
- **SCA:** Stored Communication Act (Part of ECPA) privacy from unauthorized access or interception on electronic channel.
- **SOX:** Act. Administered by Securities and exchange commission.

**Exam tip: It doesn't tell how to store records. It means which record are to be stored and for how long.*

- **Australia and New Zealand:** Data transfer outside Australia and New Zealand is prohibited until and unless proper protection is there (Similar to EU).

Australia Privacy Principles:

- Collection
- Use
- Disclosure
- Access
- Correction
- Identification

APP8: Cross Border disclosure of personal information

APP11.1: Security of personal information

- **Russia:** Russia has its own data protection law
- **Switzerland:** In line with EU law

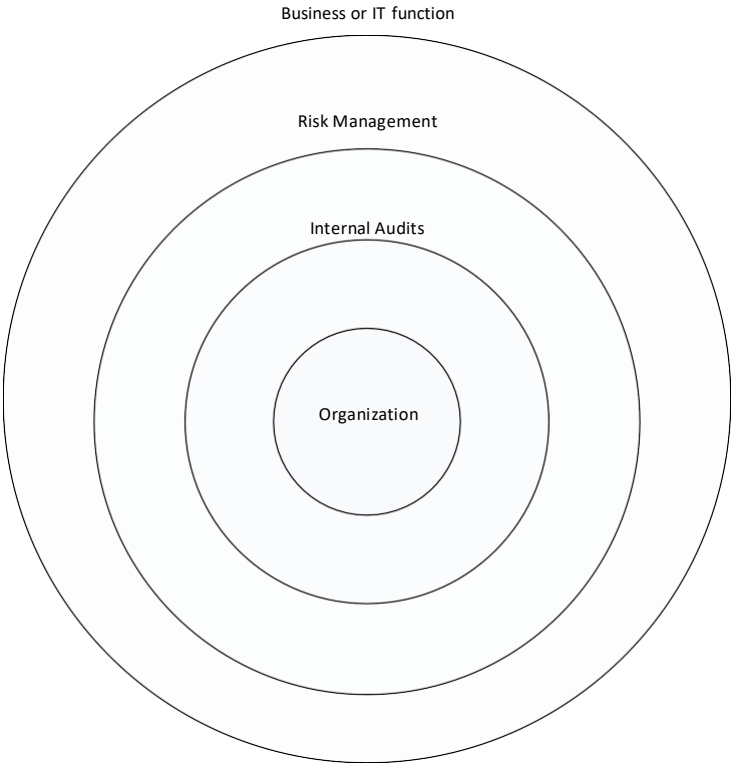
Data Processing by Third Parties:

Data controller is responsible for data processing even if its processed by Third party. Data controller is legally responsible for data security

Auditing the Cloud:

Internal and External Audits:

- Internal audits can be audited by external auditors. Internal control is the scope for External audit
- Internal audit can evaluate the organization's risk considering cloud in mind



Line of Defense for organizations

Types of Audit Reports:

**Exam tip: CSP is not comfortable sharing audit logs as it might contain other tenants' details.*

SOC1: Audit on internal control over financial reporting

SOC2: Relevant to 5 Trust principles - Security, Availability, Processing Integrity, Confidentiality, and Privacy

Examination of the design and effectiveness of Controls:

Type 1: Point in time and design of the controls

Type 2: Design and operating effectiveness of controls (6 months to a year)

SOC3: Similar to SOC2, its available for general users.

Assuring Challenges of the Cloud and Virtualization:

- Understand the Virtualization management architecture
- Verify systems are up to date and hardened according to best practice standards
- Verify the configuration of hypervisor according to organizational policy

Information Gathering: Should be a repeated process in line with PDCA process

Audit Scope:

- **Audit Scope Statement**
- **Audit Scope Restrictions:** Ensuring the operational impact of the audit would be limited
- **Gap Analysis:** Benchmarks and identifies relevant gaps against specified frameworks or standards. Performed by people who are not part of the audit scope

Audit Planning:

Define Audit Objective → Define Audit Scope → Conduct Audit → Refine the Audit Process

Standard Privacy Requirement (ISO/IEC2 7018):

- **Consent:** CSP must not use personal data they receive for any other purpose than what is intended
- **Control:** Customers have explicit control over data
- **Transparency:** CSP must inform customer about where their data resides etc.
- **Communication:** Customers should be notified for any incident
- **Independent and Yearly Audit:** CSP must go through yearly Third party Audits

Internal ISMS:

- Value of ISMS
- ISO 27001:2013 domains
- Repeatability and Standardization

Implementing Policies:

Organizational Policies: Forms the basis of functional policies that can reduce the likelihood of the following:

- Financial loss
- Irretrievable loss of data
- Reputational damage
- Regulatory and legal consequences
- Misuse and abuse of systems and resources

Cloud Computing Policies:

- **Password Policies –** Organization policy should be replicated for CSP
- **Remote Access –** MFA for CSP Admins
- **Encryption:** Check CSP policy if it matches with organization policy
- **3rd Party Access –** logging of Third party access
- **SOD –** Can it be enforced in Cloud?
- **Incident Management –** Can this be implemented with CSP?
- **Data Backup –** Is data backup included in the cloud policies?

Identifying and Involving the Relevant Stakeholders:

It's important to involve stakeholders as it forms a blueprint to identify potential impacts

**Exam tip: Risk Management in cloud computing is a joint provider and customer activity; full accountability remains with the customer.*

Impact of Distributed IT Models:

Components which does not negatively influence distributed environment

- Clear Communications: Face to face or direct communication, e.g., email, messenger
- Coordination and management activities
- Governance of process activities
- Coordination is key
- Security reporting

Understanding the implications of the cloud to enterprise Risk Management

- **Risk Profile:** Determined by the Organization's willingness to take the risk and the threats to which it is exposed
- **Risk Appetite:** How much risk an organization can accept
- **Data Subject:** Individual with personal data
- **Data Controller:** Determines the purpose and manner that the personal data will process
- **Data Processor:** Processes data on behalf of data controller
- **Data Standards:** Responsible for data content, context
- **Data Custodian:** Responsible for safe custody, transport, data storage, and implementation
- **Data Owners:** Owns the data (have legal rights)

Service Level Agreement: Contract signed between customer and CSP stating the guaranteed service being offered. If fails, financial stipulation is invoked (CIA).

SLA Component:

- Uptime guarantee

- SLA penalties
- SLA penalty Exclusion {what all things are excluded}
- Suspension of Service
- Provider liability
- Data Protection Requirement
- Disaster Recovery
- Security Recommendations

Key SLA element:

- Assessment of risk environment
- Risk Profile
- Risk Appetite
- Responsibilities
- Regulatory Requirement
- Risk Mitigation
- Risk Framework

Risk Mitigation: Mitigation of risks reduces the exposure to a risk or the likelihood of its occurring

Different Risk Frameworks:

- ISO 31000:2009 (Risk Management)
- European network and Info Sec Agency (ENISA)
- NIST

Vendor Management:

- Understanding your risk exposure
- Accountability of Compliance – It's with customer
- Common Criteria Assurance Framework – ISO 15408:2009
- CSA STAR – Provides granular level details with controls specifically defined to address the differing categories for cloud services
    - Level 1: Self-Assessment
    - Level 2: Attestation Third party
    - Level 3: Ongoing monitoring certification

Contract Management: It is important to capture the responsibilities in the contract to have clear accountability.

Supply Chain Management (ISO 28000:2007): Keep BCDR mindset.

Exam Essentials

- Various laws of countries like Canada, Australia, EU, APAC
- GDPR (Rights of data subject, Roles of Data Privacy Officer)
- PCI-DSS
- COPA, FERPA
- Preparing contractual agreement to assist both customer and CSP

Copyright Credits

1. Certified Cloud Security Professional CBK 2nd Edition by Adam Gordon.

2. Shared responsibility metrics: https://cloudsecurityknowledgesharing.com/dealing-with-shared-responsibility-model-in-public-cloud/

3. Air Management in data center: https://www.upsite.com/blog/helping-your-data-center-breath-easier-with-good-air-flow-management/