Objective of the cloud – shift from CapEx to OpEx

Risk – Threat coupled with a vulnerability.

Data life cycle – Functions, Actors, Controls

Application broken down by – Data, Functions, and processes

27001 – ISMS policy

27002 - Controls

27017 – Cloud Security

27018 – Privacy

27034 – Software/Application security

27050 - Forensics

31000 – Risk management

800-39 – Risk Management

800-40 - Patch Management

800-92 – Log capture and management

800-145 – Definition of cloud computing

800-146 - Describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides guidelines and recommendations

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.

**Software as a Service (SaaS)** - The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, **with the possible exception of limited user specific application configuration settings.**

**Platform as a Service (PaaS) -** The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but **has control over the deployed applications and possibly application hosting environment configurations.**

**Infrastructure as a Service (IaaS) -** The consumer does not manage or control the underlying cloud infrastructure but **has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).**

Safe Harbor: US Department of Commerce and EU Privacy Shield replaced Safe Harbor.

The two layers of the OSI Model abstracted from the cloud model are Session and Presentation.

AICPA relates to SOC

SOC - Service Organizational Control

SOC Type 1 – Point in time description and suitability of design of controls. PIT is 1 POT is 2 (Think alphabetical order)

SOC Type 2 is over a period of time and suitability of design and operating effectiveness of the controls. PIT is Type 1 POT is Type 2 (Think alphabetical order)

SOC 1 - Financial  
SOC 2 – Security, Availability, Processing Integrity, Confidentiality, and Privacy (Think of CSA and PP).

SOC 3 – General Use and Public

SOC 3 - Kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider.

Auditing – Define audit objectives, then audit scope, conduct audit, and refine audit/lessons learned.

GAPP – Generally accepted privacy principles

GAAP – Generally accepted accounting principles

EAR - U.S. Commerce Department controls on technology exports. (Export Administration Regulations)

ITAR - U.S. State Department controls on technology exports. (International Traffic in Arms Regulations)

Common Criteria or CC is international set of guidelines and specs for evaluating IS products to ensure they meet security standards for gov entities. Verified by vendor neutral 3rd party.

CSA Star Ratings – Level 1 is self-assessment Level 2 is Attestation which is release of assessment carried by 3rd party Level 3 is Ongoing Monitoring Certification with release of results secure property monitoring based on CTP.

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

**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 Custodian: Responsible for safe custody, transport, data storage, and implementation

• Data Owners: Owns the data (have legal rights)

Trade secret - Intellectual property protection for a confidential recipe, design, etc.

Copyright - Intellectual property protection for the tangible expression of a creative idea.

With SaaS providing a fully functioning application that is managed and maintained by the cloud provider, cloud customers incur the least amount of support responsibilities themselves of any service category.

Data analytics modes – Datamining, Agile business intelligence, Real-time analytics.

Data owner or the cloud customer is ultimately responsible for the data and compliance.

Cloud carrier – Intermediary providing connectivity and transport of cloud services between provider and consumer.

Gap analysis – benchmarks and identifies relevant gaps against frameworks or standards.

SSO - Multiple applications over a single set of credentials.

Reservations - Ensure that a minimum level of resources will always be available to a cloud customer for them to start and operate their services. **In the event of a DoS attack against one customer**, they can guarantee that the other customers will still be able to operate.

Shares – Prioritize hosts in cloud environment using a weighting system. Prevents resource contention.

Cloud orchestration – Receiving, fulfilling, managing, monitoring, and metering customer services across all data centers, AV zones, and regions.

Cloud provisioning – Deployment of a company’s cloud computing strategy. Determines services in the public cloud and which will remain on site.

Application - Responsibility would be shared between the cloud customer and cloud provider within Software as a Service

Maintenance mode requires - Remove all active production instances, Ensure logging continues, and Prevent new logins.

Management Plane Breach – Most significant risk in a managed cloud environment.

Object storage – Contains metadata that allows easy access from the web.

Enterprise risk management – Process and structures used in managing enterprise risk.

SDN – is a form of direct management, not indirect.

Application virtualization - Concept of isolating an application from the underlying operating system for testing purposes.

Sandbox - Isolated space where untested code and experimentation can safely occur separate from the production environment.

Supply chain: ISO 28000

Strategic - partners may be the fewest in number but they are the most critical to the success of the buying organization

Tactical - focuses, instead, on processes and procedures that can save time and money while also meeting customer demands and providing value

Commodity – Common goods and resources

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

Distributed resource scheduling – Used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes.

**Recovery service level (RSL)** measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation. The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan.

A generator transfer switch should bring backup power online before the UPS duration is exceeded.

Cloud provider is usually data processor and the cloud customer is the data controller.

Cloud washing - Deceptive practice where cloud is used for a non-cloud service.

In the cloud motif, the **data processor is usually the cloud provider**.

Masking – Obscures content but not format.

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:o Random substitution: HELLO → H3!!0

o Algorithmic substitution: Values are replaced based on an algorithm

o Shuffle: Shuffles different values from the dataset

o Masking: 1234 xxxx xxxx 4321

**Data Anonymization:** It is a technique for information sanitization with an intent to protect privacy.

o Direct Identifier: Such as Name, e-mail, phone number and other PII (protected by

masking).

o Indirect Identifier: Such as demographic information, dates, events. (protected by

anonymization).

**Tokenization:** Substituting sensitive information with non-sensitive information

REST – Uses URIs for web requests. It relies on stateless, client-server, and cacheable comms.

Cybersecurity activities – identify, protect, detect, respond, and recover

SNAPshots cannot take patches

IAM efforts are typically regulation driven

Encryption is always safe for data disposal in the cloud.

X509 is used for TLS and SSL for HTTPS and defines the format for PKI

X500 – LDAP

Object storage is flat and Database is hierarchal.

Cloud Broker – Provides service intermediation, aggregation, and arbitrage.

Logical Design: Part of the Design phase in SDLC

o It lacks technology detail and standards

o It communicates with abstract concepts (network, routers, system)

Physical Design: To show the hardware used to deliver the system

o Created from logical design

o Expands element from logical design

CSRF – Think cookies

XXS – Invalid input from untrusted data

Injection attack is where a malicious actor will send commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries

TLS and IPSec can be used to prevent eavesdropping.

TLS record protocol – Ensure connection is private and reliable.

TLS handshake protocol – Negotiates encryption algorithm and keys before data sent or received.

FIPS 140-2 Tested by an independent lap. Has 4 levels. Level 4 zeroizes data if compromised.

Level 1 has No specific physical security mechanisms are required.

Level 2 shows evidence of tampering, has tamper-evident coatings/seals that must be broken to attain physical access to the cryptographic keys and critical security parameters (CSPs) in module, or resistant locks on covers or doors.

Level 3 - Physical security mechanisms required at Level 3 are intended to have a high probability of detecting and responding to attempts at physical access. Tamper-detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors.

Level 4 – Highest level. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.

**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
  + Infinity Paradigm
* National Fire Protection Association (NFPA):
  + Requirement for temperature, emergency

Tier 3 – Concurrently managed

Tier 4 – Fault tolerant

* 2N+1

CSA describes relationship between the provider and the customer.

SLA - A cloud SLA (cloud service-level agreement) is an agreement between a cloud service provider and a customer that ensures a minimum level of service is maintained.

OLA – SLA negotiated between internal business units.

BCM – Defined as a holistic management approach that identifies potential threats to an org and the business impacts. Ensuring that mission critical systems are able to be restored to service following a disaster.

Release and deployment management needs to be tied to change management, config management, and problem management.

Config management - Needs to be tied to change management.

Software Development Life cycle – Planning and Requirements, defining, designing, developing, testing, and maintenance.

Verification and validation should occur at each stage of the SDLC.

Puppet and Chef can help during the secure operations phase.

Application Virtualization – encapsulation of application software execution, not emulation

NIDS – Should be deployed on the segment being monitored.

Vendor scorecard – Provides ranking of vendors based on risk.

DLP – Uses media-present checks for IP data.

Network based or gateway DLP the engine is deployed near the org gateway to monitor outgoing protocols like HTTP, HTTPS, and SMTP. For data in use it is on the user’s workstation or endpoint.

Biggest challenge for protecting data at rest with DLP is resource pooling.

Logical Design – Lacks specific details such as technologies and standards with general focus. Communicates abstract concepts such as routers and switches without detail.

Physical Design – Created from logical design. Often expands elements found in logical design.

DNSSEC – set of DNS extensions that provide authentication, integrity, and authenticated DOE for DNS data.

Risk Management Process – (FARM) – Framing, Assessing, Responding, and Monitoring

Restatement of Law - Uses relevant factors of applicable law

Doctrine of Proper Law – Addresses jurisdiction

\*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)

Threat modeling – To determine any weaknesses in the app and the potential ingress, egress, and actors before the weakness is introduced in production.

OWASP Dependency-Check – Tool that identifies project dependencies and checks whether there are known or disclosed vulnerabilities.

STRIDE – Spoofing, Tampering, Repudiation, Info disclosure, Denial of service, and elevation of privilege.

Dread

* **D**amage – how bad would an attack be?
* **R**eproducibility – how easy is it to reproduce the attack?
* **E**xploitability – how much work is it to launch the attack?
* **A**ffected users – how many people will be impacted?
* **D**iscoverability – how easy is it to discover the threat?

API Gateway – filters API traffic. Proxy or application stack focused

SIEM can help prevent escalation of privilege

DLP aids in BC/DR efforts. Can also help in the legal task of data collection.

**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

o Configuration Management: Components in cloud may not be IPsec compatible

o Performance: There is a slight degrade in performance

TPM – Full disk encryption capability. Integrity and authentication to boot process. Has unique RSA key burned into it.

HSM – Manages, generates, and stores crypto keys. Can be added to a system or network. Can’t be added if not shipped with one. Review of HSMs are done by an independent lab.

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.

DAM – Can help prevent SQL based attacks

XML GTW – Can be a reverse proxy and perform content inspection.

Data Center needs to be between 64 and 81 degrees. Thermostat on return air may result in high energy costs

Data center needs to be between 40 and 60 percent humidity. Too low increases static, too high increases corrosion and bio creep.

Release management vs change management – Release Management involves planning, coordinating, executing, and validating changes and rollouts to the production environment.

Change management - higher-level component than release management and also involves stakeholder and management approval, rather than specifically focusing the actual release itself.

Deployment management is similar to release management, but it's where changes are actually implemented on systems.

Cloud service operations manager - Responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

Core components to an encryption system architecture – Encryption Engine, Data, Keys

Privacy shield is voluntary for non-EU entities. It replaces the Safe Harbor Act. Tied to the Department of Commerce. Federal Trade Commission is enforcement body.

WORM - Long term storage written to once is and for read operations.

GLBA - IS program is critical component. Tied to financial orgs and privacy of customer info.

AICPA is tied to SOX Act.

UPS – Needs to last long enough for graceful shutdown

Portability – Addresses between one cloud provider and another or between public and private environments.

Data masking – Similar, inauthentic dataset used for training and software testing.

Identification establishes user accountability for actions on a system

Authentication – Authorization – Access are the 3 steps in order. Think of this in alphabetical order

Authentication – Identifies individual and ensures who he/she is

Authorization – What access does the individual have

Federated SSO – For facilitating inter org and inter security domain access leveraging federated identity management

Federation – An association of organizations that come together to exchange info about users and resources for collaboration and transactions

SSO – Allows a user to multiple apps with a single set of credentials.

SAML – XML based framework. Allows business to make assertions on identity, attributes, and entitlements

WS-Federation – “Defines mechanism to allow different security realms to federate such as authorized access to resources”

OpenID – “Lets developers authenticate their users across websites and apps”

OAuth - “Enables 3rd party application to obtain limited access to an HTTP service” - behalf of resource owner, or by allowing 3rd parties to obtain access on own behalf

WAF – Layer 7 FW that can understand HTTP traffic. Useful against DoS attacks

DAM – Layer 7 monitoring that understands SQL. Can stop malicious commands from being executed.

XML GTW – Transforms ways services and data is exposed as APIs to developers. Can provide AV and DLP sec controls

API GTW – Filters API traffic. Can be installed as a proxy or part of app stack

**TLS** – provides privacy/security, and integrity. Is successor to SSL. Asymmetrically sends symmetric key

Record protocol of TLS performs the authentication and encryption of data packets, and in some cases compression as well.

**SSL** - Establishes encrypted link between web server and browser.

Symmetric is a single key and asymmetric uses dual-key pair

Symmetric encryption involves a shared secret

Database activity monitoring (DAM) – Can be Host-based or Network-based

Cross-site scripting - involves the sending of untrusted data to a user's browser to be executed with their own credentials and access.

XML firewall - Most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. An XML firewall is intended to validate XML before it reaches the application.

Tokenization – Used to satisfy PCI-DSS requirements. Uses token or string of characters to substitute sensitive data that is stored.

Masking - Keeps the form but alters the content. Can be used for testing inauthentic data sets.

MTD – Focused on point in time after the outage

CSA CCM – Provides a good list of controls required by multiple compliance bodies.

Shadow IT is money spent on tech to acquire services without IT knowledge or dollars.

APIs are REST or SOAP

API programming optimizing XML request is done by SOAP

Gateways are application layer

Storage controllers – distribute workloads to each server, manage the transfer, and provide access to all files regardless of physical location

Comparing OSI and Cloud Model the session and presentation layers are abstracted.

SaaS stores CDN content PaaS is structured and unstructured IaaS is volume and object

Key capability or characteristic of PaaS – Ability to reduce Lock-In.

RTO – Think of amount of time and RPO as amount of data

Certification - Accreditation - and then operation

General server security – 800-123

UPS – Should last long enough for a graceful shutdown

Hot aisle containment - backs of servers where exhaust air is facing the backs of the over servers/devices

REST – Software architecture style of guidelines and best practices for scalable web services - Supports many formats and uses HTTP - Faster

SOAP – protocol specification for exchanging structured info in the implementation or web services - It only supports XML – Slower

Forklifting – Process of migrating entire app the way it runs in a traditional environment with minimal code changes. NOT ALL APPS ARE CLOUD READY

When dealing with EU nations then the answer should be private cloud over the other deployments

Tiers of zones: Data center then availability zones and then regions

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 (Write Once Read Many).

**Problem Management:** Objective is to minimize the impact of problems on the organization.

o A problem is the unknown cause of one or more incidents, often identified as a result of multiple similar results.

o A known error is identified the root cause of a problem.

o A workaround is a temporary way of overcoming technical difficulties.

ALE=SLE x ARO

Methods of data discovery – Label, Content, and User based.

Type 1 Hypervisor – More secure and “bare metal” - With a Type 1 hypervisor, the management software and hardware are tightly tied together and provided by the same vendor on a closed platform. This allows for optimal security, performance, and support. The other answers are all incorrect descriptions of a Type 1 hypervisor.

Type 2 Hypervisor – Less secure and depends on OS

Event - defined as a change in state that has significance for management of IT and an incident is defined as an unplanned interruption to an IT service or reduction in policy.

Incident management – Restore service as quickly as possible. Minimize adverse impact. Ensure availability and quality are maintained.

Incident classification - Priority = Urgency x Impact.

Incident management process – Incident then report then classify then investigate and collect data then resolution with approval and then implement changes

Problem – Unknown cause of one or more incidents and a known error is the root cause of a problem. A workaround is a temp way of overcoming a tech difficulty.

Utility is functionality of product.

Warranty is assurance the product will meet requirements.

ONF to ANF – One to many relationship. ONF used to create multiple ANFs.

ONF – Framework of containers for all components of app security……leveraged by the organization.

There is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization).

Therefore, the ANF is a subset of the ONF.

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

WS-Security specifications, as well as the WS-Federation system, are built upon XML, WDSL, and SOAP. SAML is a very similar protocol that is used as an alternative to WS.XML, WDSL, and SOAP are all integral to the WS-Security specifications.

Converged networking model – Optimized for cloud deployments and underlying storage. Maximizes benefits of a cloud workload

ASMP 5 steps: Specifying app requirements, Assessing risks, Creating and Maintaining ANF, Provisioning and operating, Auditing the security (SAC PA)

Proxy federation could use a 3rd party to optimize compliance with security governance

Dynamic software testing – uses Path coverage and not code or user coverage. Is also done in a runtime state.

DAST – Considered black box. Looks at execution paths and in a running state. (See above)

RASP – Focuses on apps that that have self-protection capabilities in runtime environments. Works without human intervention in response to attacks.

SAST – Generally considered white box test. Inspects the code and can help against XSS, SQL injection, and buffer overflows.

Vulnerability scans depend on vulnerability signatures

Mobile number is considered PII in EU but not US

Data archiving is tied to BC/DR

Broken authentication and session management – Avoid using custom authentication schemes.

Synthetic performance monitoring better than real time user monitoring because it is more comprehensive

Chicken coop datacenter – Long side facing the prevailing wind to allow for natural cooling.

BISCI – Covers cabling design and installation

IDCA – Covers data location

Uptime institute – Tier 1 is Basic Data Center Structure Tier 2 is Redundant Site Infrastructure Tier 3 is Concurrently maintainable Tier 4 is Fault-tolerant

Raised floors need to be 24 inches.

Hot aisle has backs of racks facing each other and Cold aisle has back of racks facing away from each other and cold air flowing between the intake side

4 9s or 99.99% – 52.56 minutes of downtime per year

5 9s or 99.999 – 5.26 minutes of downtime per year.

RSL - Refers to the percentage of production level restoration needed to meet BCDR objectives.

HA is loosely coupled and Fault tolerant is tightly coupled.

• 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).

• Static Application Security Testing (SAST):

o White box testing. Done without executing the application.

o Determines coding errors. Early development life cycle.

o Useful for XSS, SQL Injection, Backdoors.

• Dynamic Application Security Testing (DAST):

o Black box testing. Done at the runtime.

o Useful to test exposed HTTP and HTML Interfaces.

• Runtime Application Self Protection (RASP):

o Considered to focus on application that possesses self-protection capabilities. Prevents attacks by self-protecting without human intervention.

**GDPR** – General Data Protection Regulation. European Union. Based on 7 principals

**PIPEDA** - Personal Information Protection and Electronic Documents Act. Canada

**COPPA** - Children's Online Privacy Protection Act. US. FTC in 1998

**APEC** – Asia Pacific Economic Cooperation

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.

Portability - The most important cloud concept when considering BCDR planning.

iSCSI – Protocol that uses TCP to transport SCSI commands. For TCP/IP network infrastructure as a SAN. Makes block devices available via the network. Local area tech.

iSCSI - Subject to oversubscription. Should use a dedicated LAN for traffic. It is transmitted unencrypted so use only on trusted networks. It does support IPSec/IKE.

iSCSI Supports Kerberos authentication. SRP and CHAP as well.

NAS – Presents devices at a file level.

SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

A host intrusion detection system (HIDS) monitors network traffic as well as critical system files and configurations.

Security requirements should be incorporated into the software development lifecycle (SDLC) from the earliest requirement gathering stage and should be incorporated prior to the requirement analysis phase.

Measured service - most attractive aspect of cloud computing for use with BCDR.

Virtualization makes it very difficult to perform repeat audits over time to track changes and compliance.

Object storage - Typically used to house virtual machine images that are used throughout the environment.

Volume and object storage – Used when the cloud customer is responsible for deploying all services, systems, and components needed for their applications.

Inter-cloud provider - Manages memberships in federations and the use and integration of federated services.

Systems staff (not cloud customer or developer) would be responsible for implementing IPsec to secure communications for an application.

Operating system of the host controls the formatting and security settings of a volume storage system within a cloud environment.

Homomorphic - Experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first.

**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.

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 organization’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)

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 o VM is offline → can still be attacked, malware infections due to the unavailability of patching

Infrastructure as a Service

Consumer CSP

OS Storage

Software Network

Host Firewall Processing

Software as a Service

Consumer CSP

Data Infrastructure

Network, storage

OS,Servers, Application

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.

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

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:

o Physical loss or theft.

o External admins accessing the data.

o Snapshot of storage level backups being taken and removed from the system.

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.

**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.

**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 Qualities**

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.

**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

**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.

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

\*APIs allow automation of controls tasks.

**Virtualization Risks**

• 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

Configuration management tracks and maintains detailed information about all IT components within an organization. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

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.

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

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

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.

Data security and GRC are always customer responsibility.

**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.

**Federation Standard**

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

SAML is also standard for exchanging authentication and authorization data between security domains.

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. Usually used by Universities.

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