Cloud Objective – Shifting CapEx to OpEx allows enterprise to match capacity to need, as well as pay as they go for only the services that they use.

What are the types of cloud **migration strategies**?

"six R's of migration,":

1. **Rehosting** ("lift and shift")
Involve lifting your stack and shifting it from on-premises hosting to the cloud. You transport an exact copy of your current environment without making extensive changes for the quickest ROI. This is the riskiest because of risk on integration.

2. **Replatforming**
As a variation on the lift and shift, replatforming involves making a few further adjustments to optimize your landscape for the cloud. Again, the core architecture of applications stays the same.

3. **Repurchasing**
This means moving your applications to a new, cloud-native product, most commonly a SaaS platform (for example, moving a CRM to Salesforce).

4. **Refactoring**
Refactoring (or rearchitecting) means rebuilding your applications from scratch. This is usually driven by a business need to leverage cloud capabilities that are not available in your existing environment, such as cloud auto-scaling or serverless computing. Refactoring is generally the most expensive option, but also the most compatible with future versions.

5. **Retiring**
Once you have assessed your application portfolio for cloud readiness, you might find some applications are no longer useful. In this case, simply turn them off.

6. **Retaining**
For some organizations, cloud adoption does not yet make sense. Are you unable to take data off premises for compliance reasons? Perhaps you are not ready to prioritize an app that was recently upgraded? In this case, plan to revisit cloud computing at a later date. You should only migrate what makes sense for your business.

**Cloud security risks**

- **Distributed** - Laws vary across jurisdiction
- **Multitenant** - Shared physical resources make incident response, forensics, destruction, etc difficult
- **Responsibility cannot be transferred**; customer is still legally liable for the protection of the resources. Data owner maintains responsibility in all cloud models
- **Privacy** - The degree of privacy enforcement must be specified in SLA
- **CSA** may have higher requirements than the enterprise

The main difference between traditional and cloud computing is **virtualization** borne out of abstraction

**Management Plane** – APIs that are remotely accessible and those wrapped into a web-based user interface Manage

- Most significant risk in a managed cloud environment.

Can manage the VMs or virtualized services. APIs and web consoles are the way the management plane is delivered. Cloud providers and platforms will also often offer Software Development Kits (SDKs) and Command Line Interfaces (CLIs) to make integrating with their APIs easier

**Secure the Management Plane via IAM**

Both providers and consumers should consistently only allow the least privilege required for users, applications, and other management plane usage.

All privileged user accounts should use multi-factor authentication (MFA). If possible, all cloud accounts (even individual user accounts) should use MFA. It's one of the single most effective security controls to defend against a wide range of attacks. This is also true regardless of the service model:

The three main considerations from a security perspective for local access to cloud data center are physical access through KVM (keyboard, video, mouse), console access through the hypervisor, and Remote Desktop Protocol (RDP).

Regardless of which type of local access is used, multifactor authentication should be employed wherever possible, and comprehensive logging and auditing programs should be in place as well, all conforming to best practices for systems and security protection.

Exposing RDP to the Internet or outside a protected network is something that should never be done. It is an insecure protocol that will open systems to major vulnerabilities. It should always be secured behind other mechanisms such as a virtual private network (VPN).

**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 control 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**: Lose control of the amount of content on your image store
    - **VM sprawl** is defined as a large amount of virtual machines on your network without the proper IT management or control. For example, you may have multiple departments that own servers begin creating virtual machines without proper procedures or control of the release of these virtual machines

**Application plane** – layer consisting of plenty of vendors and third-party applications.
**Infrastructure plane** – layer in which all types of devices and resources from different vendors are interconnected
**Metastructure** - Connects the infrastructure to other layers
**Cloud Control plane** – layer where the data center is the component element
**MFA** is just as important for SaaS as it is for IaaS

Key techniques to create a cloud:

- **Abstraction** – abstract resources from the underlying physical infrastructure to create pools
  Hypervisors – virtual machines
  SDN – virtual network
  Storage abstraction – SAN/NAS away from physical hard drives to make larger pools.
- **Orchestration /automation** – coordinate use of resource in the resource pool. Used to provision/deprovision/resize resource automation

  Note: These orchestration/automation techniques create the essential characteristics to define "cloud."

Within a cloud environment there are two main network models, with the appropriate model dependent on the particular needs and configurations of the cloud environment.

- The **traditional networking model** has physical switches combined with virtual networks at the hypervisor level.
    - can use regular security networking tools
- The **converged networking model** combines the storage and date/IP networks into one virtualized design and is intended for use with cloud environments. Optimized for cloud deployments, the underlying storage and IP networks are combined so as to maximize the benefits of a cloud workloads.
    - Will use completely virtualized tools.

Due to the nature of a traditional networking model and the combination of physical and virtualized systems, there can sometimes be a disconnect between the two as it relates to full visibility with the virtualized networks.

The **converged networking model**, being designed and optimized for cloud usage, typically maintains better visibility and performance under cloud operating loads.

For **raw storage**, the provider enables a storage logical unit number (LUN) in the VMware server virtualization environment to be directly connected to a VM from the storage area network (SAN). Raw storage is the physical media where data is stored.

**SaaS** deployments utilize information storage and management, content and file storage, ephemeral storage, content delivery networks (CDNs), raw storage, and long-term storage.

**Ephemeral storage** is SaaS storage that exists only as long as its instance is up.

A **CDN** is SaaS storage that occurs when content is stored in object storage, which is then distributed to multiple geographically distributed nodes to improve internet consumption speed.

**Object storage** is similar to a file share accessed via APIs or a web interface. Object storage is used in IaaS deployments. IaaS also uses volume storage, in which volumes attached to IaaS instances behave just like a physical drive or an array.

**Cloud Application Management Platforms (CAMPS)** are a set of specification designed to ease management of applications, including packaging and deployment across public and private cloud platforms.

**Orchestration**: The goal of cloud orchestration is to automate the configuration, coordination, and management of software and its interaction. Receiving, fulfilling, managing, monitoring, and metering customer services across all data centers, AV zones, and regions. Used by the CSP

Orchestration can:

- Make the output of one device be the input of another
- Make one application VM start before another
- Make an application to fail to another virtualization host when the original host fails

**Cloud provisioning** – Deployment and integration of cloud computing services within an enterprise IT infrastructure. This is a broad term that incorporates the policies, procedures and an enterprise's objective in sourcing cloud services and solutions from a cloud service provider. Used by Customer.

**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.

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

**Simple Cloud Security Process Model**

- Identify necessary security and compliance requirements, and any existing controls.
- Select your cloud provider, service, and deployment models.
- Define the architecture.
- Assess the security controls.

- Identify control gaps.
- Design and implement controls to fill the gaps.
- Manage changes over time.

**Storage Area Network (SAN)** and **Network-Attached Storage (NAS)** are both common forms of storage virtualization

Containers are highly portable code execution environments. It is a virtual execution environment that features an isolated user space, but uses a shared kernel. Such containers can be built directly on top of physical servers or run on virtual machines.

Software container systems always include three key components:

- The execution environment (the container).
- An orchestration and scheduling controller (which can be a collection of multiple tools).
- A repository for the container images or code to execute.

Together, these are the place to run things, the things to run, and the management system to tie them together.

**DevOps** is a new application development methodology and philosophy focused on automation of application development and deployment. DevOps opens up many opportunities for security to improve code hardening, change management, and production application security, and even to enhance security operations in general.

**Application virtualization** — useful for sandboxing

- Wine
- Microsoft App-V
- XenApp

**Static Virtualization vs cloud computing**

Traditional Virtualization

- Abstraction of compute, network, and storage from physical infrastructure
- A human admin manually allocates resources
- Not self-service or minimal
- Not elastic due to lack of automation

Cloud Computing

- Abstraction (separating the logical resource from the underlying physical infrastructure is a major point, it allows us to create resource pools out of the underlying assets) from physical infrastructure through virtualization
- Cloud automates and orchestrates management of the resource pools
- Self-service - Users provision the resources from their own allocated pool-based on policies.

**Cloud Risk Management Tools**

The following processes help form the foundation of managing risk in cloud computing deployments.

The supplier assessment sets the groundwork for the cloud risk management program:

- Request or acquire documentation.
- Review their security program and documentation.
- Review any legal, regulatory, contractual, and jurisdictional requirements for both the provider and yourself.
- Evaluate the contracted service in the context of your information assets.
- Separately evaluate the overall provider, such as finances/stability, reputation, and outsourcers.

**Risk** – Threat coupled with a vulnerability or R * T. Sometimes Asset is part of this as R*T*A.

**Network Access Control (NAC)** is an approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement.

**Network Security Zones** - It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defense requirements.

**Network Interface Controller (NIC)** is a computer hardware component that connects a computer to a computer network. Early network interface controllers were commonly implemented on expansion cards that plugged into a computer bus.

With servers, remember the concept of applying mitigating factors where patching cannot be deployed immediately, such as temporarily disabling services or further restricting access points to services and APIs.

Having the storage traffic separated to a different LAN from application and user traffic will allow for great security and confidentiality of data transmissions.

What is **Information Gathering**?

The process of identifying, collecting, documenting, structuring, and communicating information from various sources in order to enable educated and swift decision making to occur.

What are the Information Gathering Stages?

1. Initial Scoping of Requirements
2. Market Analysis
3. Review of Services
4. Solutions Assessment
5. Feasibility Study
6. Supplementary Evidence
7. Competitor Analysis
8. Risk Review/Risk Assessment
9. Auditing
10. Contract/Service Level Agreement Review

Why is **Information Gathering** important?
To enable the selection of an appropriate service provider & effective governance on-going.

**Data life cycle** – Create, Store, Use, Share, Archive, Destroy.

Read maps to all phases. Process for create and use. Store for store and archive

- Must consider **Functions**, **Actors**, **Controls**

Data is classified based on its **value** or **sensitivity** level. This is performed in the create phase of the data lifecycle.

**Data Discovery** is a business intelligence operation and a user-driven process where data is visually represented and analyzed to look for patterns or specific attributes.

**Data Dispersion**

Pertains to how data is located and stored within a cloud environment, including how many copies are maintained, how they are geographically diverse in their location, and how redundant and available they are.the greater the degree of data dispersion, the higher the storage cost will be.

**Data Destruction in cloud**

- Overwriting is not feasible in the cloud because logical location is impossible to determine.
- Physical destruction is preferred method but not available for cloud.
- Crypto-shredding is the best method in cloud environment.

**Data Discovery Techniques**

Data Discovery is a user-driven process of searching for patterns or specific items in a data set. Data Discovery applications use visual tools such as geographical maps, pivot-tables, and heat-maps to make the process of finding patterns or specific items rapid and intuitive.

Data Discovery may leverage statistical and data mining techniques to accomplish these goals.

**Methods of data discovery** – Label, Content, and Metadata.

There are several different ways Data Discovery tools make their analysis.

- Metadata provides data its meaning and describes its attributes (the best)
- Labels provide a logical grouping of data elements and gives them a “tag” describing the data.
- Content analysis examines the data itself.
-

**Threats to Data Storage**:

- Unauthorized usage/access.
- Liability due to noncompliance.
- DoS and DDoS.
    - ○ Redundancy.
    - ○ Data Retention and Archival.
- Corruption, modification, destruction of data.
    - ○ Hashes/Digitally signed files

**Policy Controls for Privacy and Data Protection**:

- Separation of Duties.
- Training.
- Authentication and Authorization procedures.
- Vulnerability Assessment.
- Backup and Recovery process.
- Logging.
- Data-Retention control.
- Secure disposal.

**Technical Requirements** are as follows:

- Creating, accessing, updating, deleting data objects in the cloud system.
- Moving VMs and virtual appliances between cloud systems.
- Selecting the best IaaS vendor for a private externally hosted cloud system.
- Tools for monitoring and managing multiple cloud systems.
- Migrating data between cloud systems.
- Single sign-on access to multiple cloud systems.

- Orchestrated processes across cloud systems.
- Discovering cloud resources.
- Evaluating SLAs and penalties.
- Auditing cloud system.

**Preparing for legal actions**

- Legal hold When a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and ensure the preservation of relevant documents.
- E-Discovery Any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence.
- Spoilation - The intentional or accidental destruction or alteration of data either on “legal hold” or lawfully requested.
- Production Presenting the requested data to the court or requesting party

**Digital forensics** – Preserve and collect evidence from most volatile to least volatile.

Chain of evidence is a series of events that, when viewed in sequence, account for the actions of a person during a certain time period, or the location of a piece of evidence during a specified time period.

The process of Digital Forensics involves:

- Identify the incident and evidence: Primary responders goal is to preserve evidence and begin the chain of custody documentation.
- Collect the evidence: label, record, acquire evidence, ensuring that modification does not occur.
- Examine the evidence-->Data.
- Analyze the evidence -->Information.
- Report the results
- Lessons Learned.

**eDiscovery stages**

- Identification - Potentially responsive documents are identified
- Preservation - Data identified as potentially relevant is placed in a legal hold
- Collection - Transfer of data from a company to legal counsel
- Processing - Preparation for loading into a document review platform
- Review - Documents are reviewed for responsiveness to discovery requests
- Production - Documents are turned over to opposing counsel
- Presentation - Documents are displayed before audiences

**eDiscovery Investigation**

- **SaaS-based eDiscovery**:

eDiscovery software vendors host their application on their own networks and deliver it to customers via the internet. Customers use the application for various eDiscovery tasks such as analysis or review. Often perform tasks such as collection, preservation or review.

- **Host eDiscovery** (provider):

eDiscovery in cloud may mean hiring a hosted services provider to conduct it on data stored in the cloud. Customer stores data in the cloud and the vendor will do the ediscovery. The customer collects relevant data in response to an

eDiscovery matter, processes it, and sends it via the internet to their hosting provider. The provider stores customer data on their site or in a co-location facility, and runs various levels of eDiscovery on the data.

- **Third party eDiscovery**:

When no prior notification or arrangements with the CSP for ediscovery review exists, there is need for a 3rd party or specialized resources operating on its behalf. Cloud Customer may hire a third party with expertise with eDiscovery in the cloud.

Application is broken down by – **Data**, **Functions**, and **Processes**

27001 – ISMS policy, Standard
27002 - Controls
27017 – Cloud Security
27018 – Privacy on cloud
27034 – Software/Application security
27050 - eDiscovery (Forensics)
31000 – Risk management
800-37, 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

**Physical Environment of the cloud Infrastructure**

- Expensive hardware - hundreds of thousands of servers.
- Massive density of power.
- Downtime affects all dependent businesses.
    - ○ Redundancy on all levels is essential.
- Power, Pipe(cooling), Ping(connectivity) limitations.
- Temperature: Sensors will measure the heat being generated by equipment as well as the air-conditioning system's intake and discharge.
- Humidity and moisture: Sensors ensure high moisture levels won't corrode electronic elements and low levels won't cause static electricity. They also monitor for leaks in cooling equipment, pipes, etc.
- Airflow: Sensors ensure air is properly flowing through racks and to/from the air-conditioning system.
- Voltage: Sensors detect the presence or absence of line voltage.
- Power: Monitoring systems ensure proper current coming into the facility and detect failures.
- Smoke: Detection of smoke/head/flames and communication with emergency services.

With **governance** - the contract defines the roles and responsibilities for risk management between a cloud provider and a cloud customer.

**Standard Privacy (ISO/IEC 27018).**

Involves:

- Consent.
- Control.
- Transparency.
- Communications.

- Independent annual audits.

**COBIT** - Framework created by the ISACA for IT governance and management.

**ITIL** - IT Ops and support

**TOGAF** - Presentation, Application, Information and infrastructure services

**SABSA** - Business Ops support services (BOSS). A means of looking at security capabilities from a business perspective (Risk based).

**JERICHO** Model - Security and Risk management

**NERC/CIP** – Used by electric utilities.

**CWG** - Cloud working group. End user advocate.

**TCI (Trusted Cloud Initiative)** – Made by CSA and helps CSPs with identity and compliance management.

The **TCI Reference Architecture** is both a methodology and a set of tools that enable security architects, enterprise architects and risk management professionals to leverage a common set of solutions.

**GDPR – General Data Protection Regulation**. European Union.

Key provisions of GDPR include:

1. Notification of breaches,
2. New requirements for data processors,
3. Designation of DPO,
4. Accountability obligations,
5. Rules for international transfers, and
6. Substantial global sanctions (up to 4% of worldwide revenues).
7. Extension of individual right
    - Right to be forgotten
    - Right to data portability
    - Data protection by design/default

National laws compliant with EU GDPR
Switzerland, Lichtenstein, Norway, Iceland, Argentina
Australia — Privacy Act 1988, since 2014 Australian Privacy Principles
New Zealand, Japan
Canada — PIPEDA
Androrra, Israel, Uruguay

**PIPEDA** - Personal Information Protection and Electronic Documents Act. Canada
Contains various provisions to facilitate the use of electronic documents. The act was also intended to reassure the European Union that the Canadian privacy law was adequate to protect the personal information of European citizens.

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

**APEC** – Asia Pacific Economic Cooperation

Part 1: Preamble

Part 2: Scope

Part 3: Information Privacy Principles

Part 4: Implementation

**OECD** - Organization for Economic Cooperation and Development

Standards organization made up of representatives from many countries, and it publishes policy suggestions. Its standards are not legally binding and do not have the effect of a treaty or other law (such as GDPR). The OECD published the first set of internationally accepted privacy principles and recently published a set of revised guidelines governing the protection of privacy and trans-border flows of personal data.

**Privacy and Security Guidelines**

Aims to globally protect privacy through a practical, risk-management-based approach.

Should follow these principles:

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness

**Proxy-based encryption** - where you place an encryption proxy in a trusted area between the cloud user and the cloud provider and the proxy manages the encryption before transferring the data to the provider.

**Hypervisors** are not required in containerization environments.

European Network and Information Security Agency (ENISA) - Risk framework focused on cloud security.
The European NIST basically.

ENISA Cloud computing key legal issues:
1. Data protection
2. Availability and integrity
3. Minimum standard or guarantee
4. Confidentiality
5. Intellectual property
6. Professional negligence
7. Outsourcing service and changes in control

**PDCA** is (plan–do–check–act) and is also known as the Deming cycle. It is an iterative four-step management method used in business for the control and continuous improvement of processes.

Gartner defines **IAM (Identity and access management**) as "the security discipline that enables the right individuals to access the right resources at the right times for the right reasons."

Best IAM for organization's resources simultaneously on cloud & on-Prem - ABAC

**CASB** – Cloud access security broker handles identity and access management (IDM).

**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.

SaaS provider is responsible for perimeter security, logging/monitoring/auditing, and application security, while the consumer may only be able to manage authorization and entitlements.

Application responsibility would be shared between the cloud customer and cloud provider within Software as a Service.

**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).

IaaS gives patching responsibility to the cloud customer because they are responsible for the virtual machines and images.

IaaS has a number of key benefits for organizations, which include but are not limited to these:

- Usage is metered and priced on the basis of units (or instances) consumed.
- It has an ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure.
- It has a reduced cost of ownership. There is no need to buy assets for everyday use, no loss of asset value over time, and reduced costs of maintenance and support.
- It has a reduced energy and cooling costs along with "green IT" environment effect with optimum use of IT resources and systems.

**CCM** is designed to provide guidance for cloud vendors and to assist cloud customers with assessing the overall security risk of a CSP. Can be used to perform security control audits. A fundamental richness of the CCM is its ability to provide mapping and cross relationships with the main industry-accepted security standards, regulations, and controls frameworks (such as ISO 27001/27002, ISACA COBIT, and PCI DSS).

Use of insecure APIs can be reduced with proper vetting. All APIs must be vetted.

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

**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.

The two layers of the **OSI Model abstracted** from the cloud model are Session and Presentation. Layers 7, 6, and 5 are combined into Application layer,

AICPA relates to SOC and is tied to SOX Act as well
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 - Kind of SSAE audit report that a cloud customer most likely will receive from a cloud provider. General Use and Public

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

**Mapping** – Data classification process that ensures that sensitive data in one environment is treated as sensitive data in another. This is different than Labels

The integrity principle of the **EU Data protection directive 95/46 EC** states that individual must be allowed to correct any of their own information if it is inaccurate.

The data directive gives the following principles:

- **Notice** - An individual must be informed that personal information about him is being gathered or created.
- **Choice** - Each individual can choose whether to disclose his personal information. No entity can gather or create personal information about an individual without that individual's explicit agreement.
- **Purpose** - An individual must be told the specific use to which the information will be put, including sharing the data.
- **Access** - An individual is allowed to get copies of any of his own information held by any entity
- **Integrity** - An individual must be allowed to correct any of his own information if it is inaccurate
- **Security** - Any entity holding an individual's personal information is responsible for protecting that information and is ultimately liable for any unauthorized disclosure of that data.
- **Enforcement** - All entities that have any personal data of any EU citizen understand that they are subject to enforcement actions by EU authorities

Security professionals must understand the data privacy acts that will affect any PII that is stored in the cloud.

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

**SOX** – Publicly traded companies GLBA – Financial Companies

**FedRAMP** - Dictates that American federal agencies must retain their data within the boundaries of the United States, including data within cloud datacenters.

**GAPP** – Generally accepted privacy principles. Assist Certified Accountants and Certified Public Accountants in creating an effective privacy program for managing and preventing privacy risks.

- Was previously known as the AICPA/CICA Privacy Framework

**GAAP** – Generally accepted accounting principles
- A common set of accounting principles, standards, and procedures issued by the Financial Accounting Standards Board (FASB). Maintained by AICPA in the US.

**HITECH** Act - Legislation that was created to stimulate the adoption of EHR and the supporting technology in the United States.

**EAR** - U.S. Commerce Department controls on technology exports. (Export Administration Regulations)
- EAR covers the restriction of commercial and dual-use items and technologies.

**ITAR** - U.S. State Department controls on technology exports. (International Traffic in Arms Regulations)
- You can find ITAR-covered items on the USML, while EAR items are listed on CCL.

**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.

There are three steps to successfully submit a product for evaluation according to the Common Criteria:

- The vendor must detail the security features of a product using what is called a security target
- The product, along with the Security Target, goes to a certified laboratory for testing according to evaluate how well it meets the specifications defined in the protection profile.
- A successful evaluation leads to an official certification of the product

**Profile Protection**: Identifies security requirements for a class of security devices.

- Security requirements & protection.
- What customer needs (security desire).
- Products can comply with more than one PP.

**Security Targets**: Claims of security from the vendor that are built into a **TOE (Target of Evaluation**).

- The document that identifies the security properties of the TOE.
- The ST may have one or more PP's.

CC has EALs or earned assurance levels from

| Level | Assurance Level |
|---|---|
| EAL1 | Functionally tested |
| EAL2 | Structurally tested |
| EAL3 | Methodically tested & checked |
| EAL4 | Methodically designed, tested, & reviewed |
| EAL5 | Semi-formally designed & tested |
| EAL6 | Semi-formally verified, designed, & tested |
| EAL7 | Formally verified, designed, & tested |

**CSA Star Ratings**

**Level 1** is self-assessment

- Consensus Assessments Initiative Questionnaire (CAIQ) - A standard template for cloud providers to document their security and compliance controls.

**Level 2** is Attestation which is release of assessment carried by 3rd party against 27001 or CCM
**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 Owners**: Owns the data (have legal rights) Data owner or the cloud customer is ultimately responsible for the data and compliance.
**Data Controller**: Person, public authority, agency that determines the purposes and means of processing to be in compliance with laws and regulations.
**Data Processor**: Processes data on behalf of data controller (e.g., CSP)
**Data Custodian**: Responsible for safe custody, transport, data storage, and implementation

- Knowledge of the system is a major challenge for DC.

**Cloud carrier** – Intermediary providing connectivity and transport of cloud services between provider and consumer.
**Total Risk** – Risk before any control is implemented.

**Residual Risk** - Leftover risk after applying control.
**Secondary Risk** – When one risk triggers another.
**KPIs** - Examined before you meet your goals. Backward looking.
**KRIs** - KRIs examine what might cause you to not meet your performance. Forward looking.
**BIA** – Business impact analysis determines critical paths, processes, and assets of on organization.

**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.

**Maintenance mode** requires -

- Security protection and safeguards continue to apply to all hosts and VMSs when moved
- Remove all active production instances,
- Ensure logging continues, and
- Prevent new logins.

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

- Data mining is used to reveal hidden relationships, patterns and trends by running queries on large data stores.

One thing that might come up is code coverage vs path coverage - Code is static and path is dynamic

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

**DNSSEC** – Ensures fully qualified domain names (FQDNs) are validated.

NOTE: DNSSEC does not provide encryption. It also does not protect against Confidentiality and DDoS.

**Zone Signing** - Process of a client using digital signatures to validate a DNS resolution request back to an authoritative source.

Components

- Zone Signing Key (ZSK) Used to sign and validate the individual record sets within the zone.
- Key Signing Key (KSK) Used to sign the DNSKEY records in the zone.

- Locking down DNS servers and disabling zone transfers are best practices, and the use of DNSSEC will largely prevent the hijacking and redirecting of traffic because even if the DNS servers were compromised, there will be no way without the DNSSEC trust anchors established to get hosts to accept the new data.

**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.

**Limits** – Cannot be placed on a hypervisor but can be put on a customer, VM, or service.

**Application** - Responsibility would be shared between the cloud customer and cloud provider within SaaS

SaaS provider is responsible for perimeter security, logging/monitoring/auditing, and application security, while the consumer may only be able to manage authorization and entitlements.

**Maintenance mode** requires - remove all active production instances, Security monitoring continues, Ensure logging continues, and Prevent new logins.

**Rate Limiting** – Way to control the number of API requests made in a certain time frame.

4 core components of cloud computing – CPU, Disk, Memory, Network

In IaaS cloud model, **Homogenous cloud computing**, is the optimization of cloud computing and cloud services for a particular industry or specific-use application.

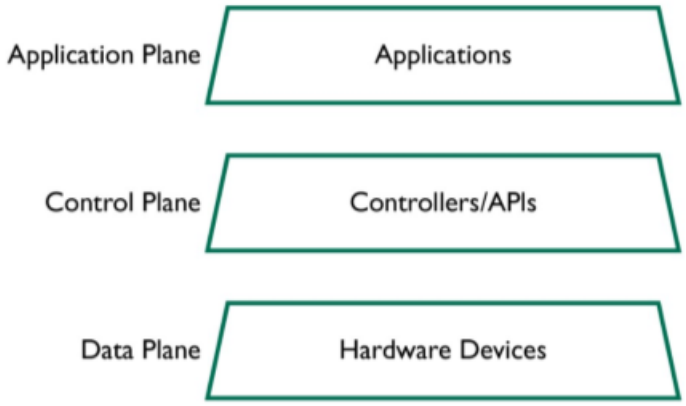
**Enterprise Risk Management** – Process and structures used in managing enterprise risk.

**Software-defined networking (SDN)** technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, making it more like cloud computing than traditional network management. SDN attempts to centralize network intelligence in one network component by disassociating the process of network packets (data plane) from the routing process (control plane).

With software-defined networking (SDN), the filtering of network traffic is separated from the forwarding of network traffic so that it can be independently administered.

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

- Network devices and the data operate at the infrastructure (data) layer,
- network services and SDN software at the control layer
- business apps at the application layer,
- APIs bridge between Application and Control layers using NBI and
- Control data plane is bridge between control and infrastructure layers.




**VLANs** are used to segregate different cloud customers or different zones within an application.

Most cloud computing today uses SDN for virtualizing networks. (VLANs are often not suitable for cloud deployments since they lack important isolation capabilities for multitenancy.)

**Software-Defined Networking (SDN**): This is an approach to networking that abstracts the hardware involved in communication away from the design and control of the overall network.

- It is typically composed of 3 aspects:
    - Data plane - where the hardware resides
    - Control plane - where the centralized controller and network intelligence engines functions, and
    - Application plane - where programs that utilize the underlying network components make their requests to the control plane, through interaction with users.

The purpose of SDN is to separate traditional network traffic (this can apply to wired or wireless) into three components: raw data, how the data is sent, and what purpose the data serves. This involves a focus on data, control, and application (management) functions or "planes" which map to the infrastructure, control and application layers.

- Application layer (Application plane) - applications which interface with the control level to specify needs and requirements.
- Control layer (Control plane) - Network services, determining how traffic should flow based on the status of the infrastructure layer (data plane) and the requirements specified by the application layer.
- Infrastructure layer (Data plane) - Network switches and routers, and the data itself as well as the process of forwarding data to the appropriate destination.

With SDN, the filtering and forwarding capabilities and administration are separated. This allows the cloud provider to build interfaces and management tools for administrative delegation of filtering configuration, without having to allow direct access to underlying network equipment.

SDN abstracts the network management plane from the underlying physical infrastructure, removing many typical networking constraints.

**Architectural components**:

- **SDN Application** (SDN App) - programs that communicate their network requirements and desired network behavior to the SDN Controller via a northbound interface (NBI).
    - SDN Northbound Interfaces (NBI) - The interfaces between SDN Applications and SDN Controllers.
- **SDN Controller** - in charge of translating the requirements from the SDN Application layer down to the SDN Datapaths (A logical network device).
    - SDN Control to Data-Plane Interface (CDPI) Southbound - The interface defined between an SDN Controller and an SDN Datapath.

- APIs bridge between Application and Control layers using **NBI** and
- **Control Data plane** is bridge between control and infrastructure layers.

**Software-defined data center (SDDC**; also: virtual data center, VDC) is a marketing term that extends virtualization concepts such as abstraction, pooling, and automation to all data center resources and services to achieve IT as a service (ITaaS).

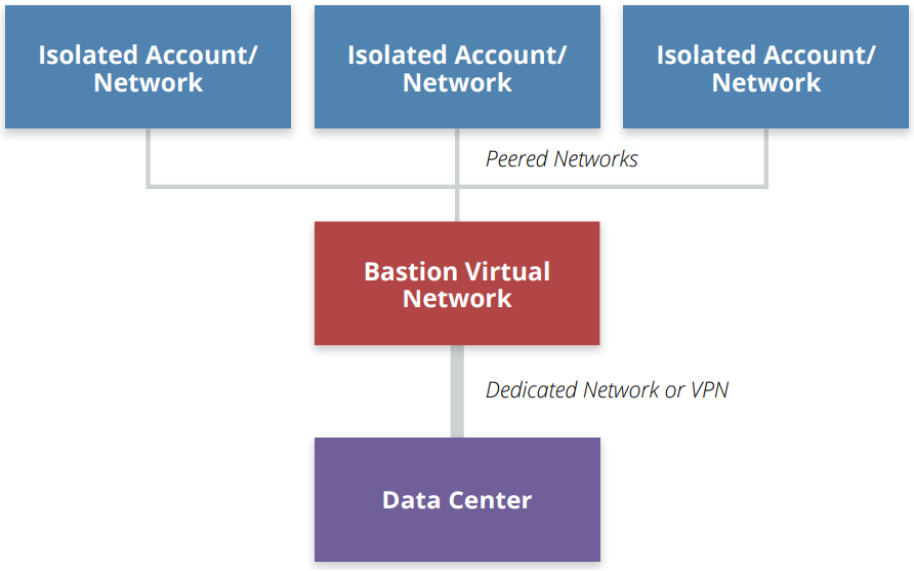
- In a SDDC, all elements of the infrastructure — networking, storage, CPU and security – are virtualized and delivered as a service.
- While ITaaS may represent an outcome of SDDC, SDDC is differently cast toward integrators and datacenter builders rather than toward tenants. Software awareness in the infrastructure is not visible to tenants.

In **hybrid cloud** considerations, the architecture for hybrid cloud connectivity is "bastion" or "transit" virtual networks. This scenario allows you to connect multiple, different cloud networks to a data center using a single hybrid connection.

- The cloud user builds a dedicated virtual network for the hybrid connection and then peers any other networks through the designated bastion network.

- The second-level networks connect to the data center through the bastion network, but since they aren't peered to each other they can't talk to each other and are effectively segregated.

Additionally, you can deploy different security tools, firewall rulesets, and Access Control Lists in the bastion network to further protect traffic in and out of the hybrid connection.




**Bastion" or "Transit" networks for more-flexible hybrid cloud architectures.**

Virtual Machines are Immutable because any patching or other changes to a running workload wouldn't change the image, and, thus, new instances would be out of sync with whatever manual changes you make on whatever is running. We call these virtual machines immutable.

To reconfigure or change an immutable instance you update the underlying image, and then rotate the new instances by shutting down the old ones and running the new ones in their place.

- Leverage immutable workloads whenever possible.
    - Disable remote access.
    - Integrate security testing into image creation.
    - Alarm with file integrity monitoring.
    - Patch by updating images, not patching running instances.
    - Choose security agents that are cloud-aware and minimize performance impact, if needed.

- Maintain security controls for long-running workloads but use tools that are cloud aware.
- Store logs external to workloads.
- Understand and comply with cloud provider limitations on vulnerability assessments and penetration testing

The primary security responsibilities of the cloud provider in compute virtualization are to enforce isolation and maintain a secure virtualization infrastructure.

Primary responsibility of the cloud user is to properly implement the security of whatever it deploys within the virtualized environment

Firstly, the cloud user should take advantage of the security controls for managing their virtual infrastructure, which will vary based on the cloud platform and often include:

- Security settings, such as identity management, to the virtual resources.
- Monitoring and logging
- Image asset management
- Use of dedicated hosting

Secondly, the cloud user is also responsible for security controls within the virtualized resource:

- This includes all the standard security for the workload, be it a virtual machine, container, or application code.
- Ensure the deployment of only secure configurations (e.g., a patched, updated virtual machine image). Due to the automation of cloud computing it is easy to deploy older configurations that may not be patched or properly secured.

**Virtualized resources** tend to be more ephemeral and change at a more rapid pace. Any corresponding security, such as monitoring, must keep up with the pace.

Host-level monitoring/logging may not be available, especially for serverless deployments. Alternative log methods may need to be implemented. For example, in a serverless deployment, you are unlikely to see system logs of the underlying platform and should offset by writing more robust application logging in to your code.

Most cloud computing today uses SDN for virtualizing networks. (VLANs are often not suitable for cloud deployments since they lack important isolation capabilities for multitenancy.)

SDN abstracts the network management plane from the underlying physical infrastructure, removing many typical networking constraints. For example, you can overlay multiple virtual networks, even ones that completely overlap their address ranges, over the same physical hardware, with all traffic properly segregated and isolated.

SDNs are also defined using software settings and API calls, which supports orchestration and agility.

A major aspect of a **virtual environment** is that servers are not physically cabled into switches and routers.

As such, if two hosts are on the same hypervisor, they can directly communicate with each other without the need to route the traffic through the physical devices.

This limits the use of physical security measures such as IDS and IPS systems, though most vendors have begun to offer virtualized appliances to mitigate this limitation.

Virtual networks move packets in software and monitoring cannot rely on sniffing the physical network connections.

To compensate, you can route traffic to a virtual network monitoring or filtering tool on the same hardware.

You can also bridge all network traffic back out to the network, or route it to a virtual appliance on the same virtual network. Each of these approaches has drawbacks since they create bottlenecks and less-efficient routing.

**Cloud providers** should:

- Inherently secure any underlying physical infrastructure used for virtualization.
- Focus on assuring security isolation between tenants.
- Provide sufficient security capabilities at the virtualization layers to allow cloud users to properly secure their assets.
- Strongly defend the physical infrastructure and virtualization platforms from attack or internal compromise.

- Implement all customer-managed virtualization features with a secure-by-default configuration.

Specific priorities:

**Compute**

- Use secure hypervisors and implement a patch management process to keep them up to date.
- Configure hypervisors to isolate virtual machines from each other.
- Implement internal processes and technical security controls to prevent admin/non-tenant access to running VMs or volatile memory.

**Network**

- Implement essential perimeter security defenses to protect the underlying networks from attack and, wherever possible, to detect and prevent attacks against consumers at the physical level, as well as at any virtual network layers that they can't directly protect themselves.
- Assure isolation between virtual networks, even if those networks are all controlled by the same consumer, unless the consumer deliberately connects the separate virtual networks.
- Implement internal security controls and policies to prevent both modification of consumer networks and monitoring of traffic without approval or outside contractual agreements.

**Storage**

- Encrypt any underlying physical storage, if it is not already encrypted at another level, to prevent data exposure during drive replacements.
- Isolate encryption from data-management functions to prevent unapproved access to customer data.

**Cloud users** should:

- Ensure they understand the capabilities offered by their cloud providers as well as any security gaps.
- Properly configure virtualization services in accordance with the guidance from the cloud provider and other industry best practices.
- The bulk of fundamental virtualization security falls on the cloud provider

- For **containers**:
    - Understand the security isolation capabilities of both the chosen container platform and underlying operating system then choose the appropriate configuration.
    - Use physical or virtual machines to provide container isolation and group containers of the same security contexts on the same physical and/or virtual hosts.
    - Ensure that only approved, known, and secure container images or code can be deployed.
    - Appropriately secure the container orchestration/management and scheduler software stack(s).
    - Implement appropriate role-based access controls and strong authentication for all container and repository management.

**Data Dispersion** is much like traditional RAID technologies; spreading the data across different storage areas and potentially different cloud providers spread across geographic boundaries.

This comes with inherent risk. If data is spread across multiple cloud providers, there is a possibility that an outage at one provider will make the dataset unavailable to users, regardless of location. This would be a threat to availability.

- SSMS – Secret sharing made short is encrypting data, splitting data in pieces, splitting the key in pieces and then signing and distributing them to various storage locations.
- AONT-RS - Integrates the AONT and erasure coding. This method first encrypts and transforms the information and the encryption key into blocks in a way that the information cannot be recovered without using all the blocks, and then it uses the IDA to split the blocks into shares that are distributed to different cloud storage services (similar to SMSS).

**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.

- Physical Sandbox – Isolation of devices and cabling. May be called air-gapped.
- Logical Sandbox – Isolated memory space where untrusted or untested code can be run in isolation.

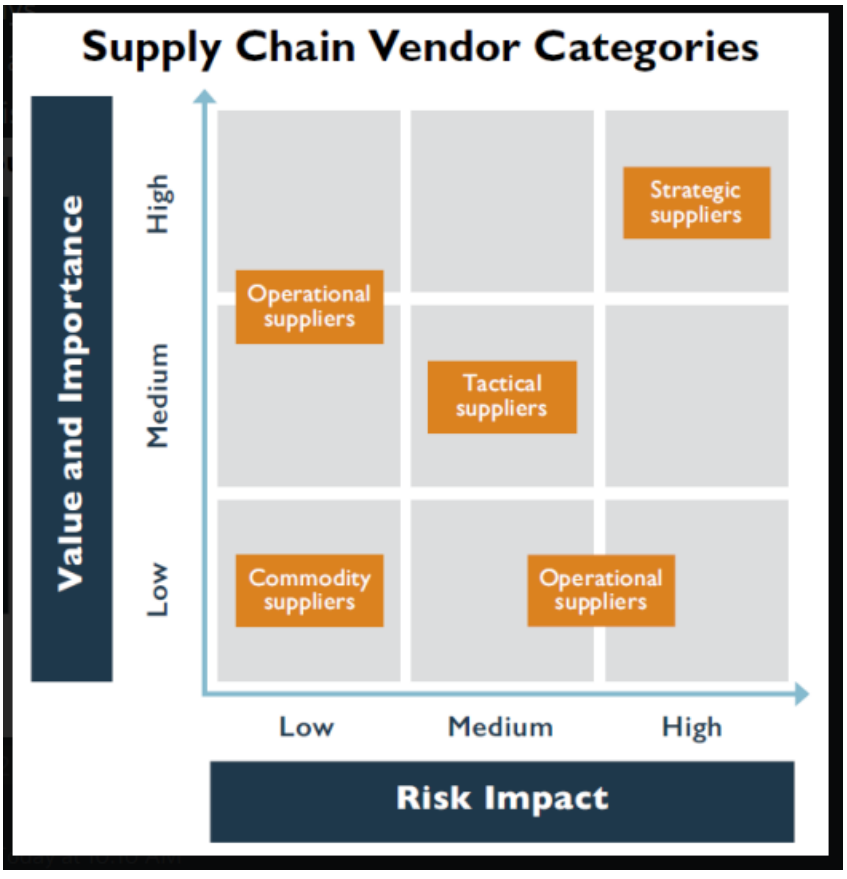
Useful for sandboxing

- Wine
- Microsoft App-V
- XenApp

Supply chain risk management practices NIST 800 - 161

**Supply chain: ISO 28000**

Categorizing or ranking a vendor/supplier on some sort of scale is critical when appropriately managing the relationship with that vendor/supplier appropriately.



**Strategic** suppliers are deemed to be mission critical and cannot be easily replaced if they become unavailable. While you will typically do business with very few of these types of partners, they are the most crucial to the success or failure of the enterprise cloud architecture.

Strategic procurement is a systematic, long term and holistic approach to acquiring current & future needs of an organization. Partners may be the fewest in number but they are the most critical to the success of the buying organization.

- Strategic (high risk, high cost & imptc) - partners may be the fewest in number but they are the most critical to the success of the buying organization

**Tactical** suppliers supplement strategic and commodity suppliers to manage emerging unforeseen issues and incidents.

Tactical procurement on the other hand is a short term, transactional activity, commonly practiced in small to medium size manufacturing organizations. Focuses on processes and procedures that can save time and money while also meeting customer demands and providing value.

- mid risk/mid cost-impt - focuses instead, on processes and procedures that can save time and money while also meeting customer demands and providing value

**Operational** Procurement deals with meeting the daily purchasing needs of organization.

- (low risk, mid-high cost/impt or
- mid-high risk, low cost/impt)

**Commodity** suppliers on the other hand provide goods and services that can easily be replaced and sourced from a variety of suppliers if necessary.

(low risk, low cost impt) – Common goods and resources

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

- Gen should have enough fuel to last 12 hours
- UPS – Should last long enough for graceful shutdown.
- UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations.

**Recovery service level (RSL)** measures the percentage of operations that would be recovered during a BCDR situation.

**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.

**Recovery time objective (RTO)** measures the amount of time necessary to recover operations to meet the BCDR plan. We want to be back up this soon. (significantly faster than MTD)

**MTTR** = Mean Time To Recovery — On average, recovery takes this long.

**MAD** = Maximum Allowable Downtime — Cannot be down longer than this. (or company fails, perhaps), aka MTD = Maximum Tolerable Downtime - Maximum time that can be continued without a resource.

Data archiving is tied to BC/DR

**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.

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

Access controls and encryption are the core data security controls

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

**Data Discovery Mechanisms**

- Metadata – Provides data its meaning and describes attributes. "Data about data"
- Labels- Provide a logical grouping of data and provides a tag to describe the data.
- Content Analysis examines the data itself.

**Data Protection by States**

Common **Protections** for **Data in Use**

- Digital signatures and encryption to protect APIs.
- IRM can be used as a means for data classification and control.
- DRM is an extension of normal data protection which is encapsulated within the concept of IRM.
- In DRM, advanced security controls such as extra ACLs and permission requirements are placed onto the data.

Common **Protections** for **Data in Motion/Transit**

- VPN (IPsec) to provide confidentiality. IPSec tunnel mode is a good solution but heavy
- TLS/SSL/HTTPS to prevent eavesdropping or tampering. SSL/TLS create an encrypted tunnel.
- All the connections from host to cloud should be encrypted in transit (TLS 1.2).
- VLANs help provide confidentiality and integrity. Separation/isolation, Transport security, VLANs
- DLP provides control between demarcation network zones by using activity monitoring and egress filtering.

TLS and IPSec are cryptographic protocols designed to secure communication over a network.

**TLS Vs IPSec**

- TLS requires a PKI. IPSec does not
- TLS is Network Address Translation (NAT) friendly , IPSec is not
- More devices support TLS than support IPSec
- TLS is more performance-intensive that IPSec. IPSec is heavy.

Common **Protections** for **Data in Use**

- Restricted access, Digital signatures and encryption to protect APIs.
- Homomorphic encryption. The idea is that if we could keep a dataset encrypted while being manipulated in memory or shared with another application, we would then never have to decrypt it, making the data transaction safer.
- IRM can be used as a means for data classification and control.
- DRM is an extension of normal data protection which is encapsulated within the concept of IRM.
- In DRM, advanced security controls such as extra ACLs and permission requirements are placed onto the data.

Common **Protections** for **Data at Rest (DAR)**

- Encryption, Redundancy
- Data stored in the database, or any repository should be encrypted (AES 256)

**Masking** – Obscures content but not format. Typically for the purpose of "testing" using replaced data

**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
- Deletion
- Algorithmic substitution: Values are replaced based on an algorithm. Allows the real data to be regenerated.
- Shuffle: Shuffles different values from the dataset
- Masking: 1234 xxxx xxxx 4321

**Data Anonymization**: It is a technique for information sanitization (masking the indirect identifier) 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. Tokenization is the practice of utilizing a random or opaque value to replace what would otherwise be sensitive data. Can be used to map back to original data. Typically needs 2 databases. Tokenization generates a token that is used to substitute sensitive data, which itself is stored in a secured location such as a database. When accessed by a nonauthorized entity, only the token string is shown, not the actual data.

**Purge** - A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratories.

**APIs are REST or SOAP**

APIs are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over HTTP/S and thus work well across diverse environments.

These can use a variety of authentication mechanisms, as there is no single standard for authentication in REST.

- HTTP request signing and OAuth are the most common; both of these leverage cryptographic techniques to validate authentication requests

**REST** – Most prevalent in web applications and relies on HTTP and supports various formats such as JSON, and XML, which is the most widely used, allows caching for performance. Software architecture style of guidelines and best practices for scalable web services -

- HTTP request signing and OAuth are the most common authentication mechanisms
- Supports many formats (JSON, XML) and relies on HTTP
- REST does not require an enduring session where a server has to store data.
- REST Uses URIs for web requests.
- It relies on stateless, client-server, and cacheable communications.

- Rest supports caching but SOAP does not.
- REST HTTP methods correspond to CRUD methods: [C]reate (POST) [R]ead (GET) [U]pdate (PUT) [D]elete (DELETE)
- Good performance and scaling - Faster

**SOAP** – Messaging specification designed for exchanging structured information in web services and operates independently of the client OS. Protocol specification for exchanging structured info in the implementation of web services

- Encapsulates information in what is known as a SOAP envelope and then uses HTTP or FTP or SMTP to transfer the data. Since everything must be "put in an envelope and addressed properly" it adds overhead.
- SOAP only supports XML formatted data and does not allow for caching.
- API programming optimizing XML request is done by SOAP.
- Lower performance and scalability compared to REST. – Slower
- SOAP relies on encryption for security……..NOT TLS or SSL.
- Message-level encryption
- SOAP allows programs to operate independently of the client operating system.
- Provides WS-* features, should only be used when REST is not available
- SOAP uses Asynchronous processing, format contracts and Stateful operations.

HTTP is over TCP and IP. SOAP is over HTTP.

TLS for REST and message-level encryption for SOAP

**SNAPshots** cannot take patches, so any VM taken out of the storage and put into production needs to be checked against configuration versions to determine if there were patches applied to the environment while it was stored.

IAM efforts are typically regulation driven

Encryption is always safe for data disposal in the cloud.

TLS is more performance intensive than IPSEC. More devices support TLS than Ipsec

A major difference between IPSec and other protocols such as TLS is that IPSec operates at the internet network layer, allowing for complete end-to-end encryption of all communications and traffic.

**Virtual Private Network (VPNs)** -

VPN security technology is used to give administrators access into trust zones within an environment.

Secure tunneling technologies are used to encrypt and protect the communications traffic, most notably with TLS.

IPsec is a protocol for encrypting and authenticating packets during transmission between two parties, i.e., pair of servers, a pair of network devices, or network devices and servers.

The protocol will perform both authentication and negotiation of security policies between the two parties at the start of the connection and then maintain them throughout its use.

A major difference between IPsec and other protocols such as TLS is that IPsec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

This also allows the encryption and security to automatically be implemented by the systems or networks and not be dependent on the application framework or code to handle encryption and security, thus releasing the application

developers from these requirements and allowing the requirements to be handled by dedicated staff that specialize in them.

Drawbacks to consider with IPsec as well.

- The first is the load that IPsec adds to systems and a network.
- Because IPsec is not implemented at the application layer, and not typical enabled or installed by default on any systems, additional effort is required by the systems or network staff to implement and maintain it.

In a cloud environment, this will be a contractual and SLA issue if desired by the cloud customer. The support issues may be extremely expensive and complex and CSP may not be willing to support at all.

**IPsec** - IPSEC Primer RFC 4301 - Security Architecture for the Internet Protocol

**Authentication** - Used informally to refer to the combination of two nominally distinct security services, data origin authentication and connectionless integrity.

- Data Origin Authentication - A security service that verifies the identity of the claimed source of data.
- This service is usually bundled with connectionless integrity service.

**Integrity** - A security service that ensures that modifications to data are detectable.

IPsec supports two forms of integrity:

- Connectionless integrity is a service that detects modification of an individual IP datagram, without regard to the ordering of the datagram in a stream of traffic.
- The form of partial sequence integrity offered in IPsec is referred to as anti-replay integrity, and it detects arrival of duplicate IP datagrams (within a constrained window).

**Confidentiality** - The security service that protects data from unauthorized disclosure. In the IPsec context, using ESP in tunnel mode, especially at a security gateway, can provide some level of traffic flow confidentiality.

**Encryption** - A security mechanism used to transform data from an intelligible form (plaintext) into an unintelligible form (ciphertext), to provide confidentiality.

**What does IPsec do?**

IPsec creates a boundary between unprotected and protected interfaces, for a host or a network. Traffic traversing the boundary is subject to the access controls specified by the user or administrator responsible for the IPsec configuration.

IPsec uses two protocols to provide traffic security services -- Authentication Header (AH) and Encapsulating Security Payload (ESP).

IPsec implementations MUST support ESP and MAY support AH. (there are very few contexts in which ESP cannot provide the requisite security services. ESP can be used to provide only integrity, without confidentiality, making it comparable to AH in most contexts.

- The IP Authentication Header (AH) offers integrity and data origin authentication, with optional (at the discretion of the receiver) anti-replay features.
- The Encapsulating Security Payload (ESP) protocol offers the same set of services, and also offers confidentiality. Use of ESP to provide confidentiality without integrity is NOT RECOMMENDED.
- Both AH and ESP offer access control, enforced through the distribution of cryptographic keys and the management of traffic flows as dictated by the Security Policy Database.

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

**Challenges with IPsec**

- Configuration Management: Components in cloud may not be IPsec compatible
- Performance: There is a slight degrade in performance. More degradation than TLS

**Security Association (SA)**

An SA is a simplex "connection" that affords security services to the traffic carried by it.

Security services are afforded to an SA by the use of AH or ESP, but not both.

If both AH and ESP protection are applied to a traffic stream, then two SAs must be created and coordinated to effect protection of the security protocols.

To secure typical, bi-directional communication between two IPsec-enabled systems, a pair of SAs (one in each direction) is required. IKE(v2) explicitly creates these SA pairs.

The set of security services offered by an SA depends on the security protocol selected, the SA mode, the endpoints of the SA, and the election of optional services within the protocol.

What about the **Authentication Header (AH)**?

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays.

AH provides authentication for as much of the IP header as possible, as well as for next level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus, the protection provided to the IP header by AH is piecemeal.

- AH may be applied alone, or in combination with the ESP, or in a nested fashion.
- ESP may be used to provide the same anti-replay and similar integrity services, and it also provides a confidentiality (encryption) service.

NOTE: The primary difference between the integrity provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP (e.g., via use of tunnel mode).

The integrity algorithm employed for the Integrity Check Value (ICV) computation is specified by the SA.

For point-to-point communication, suitable integrity algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., AES [AES]) or on one-way hash functions (e.g., MD5, SHA-1, SHA-256, etc.).

What about **Encapsulating Security Payload (ESP)**?

The ESP header is designed to provide a mix of security services in IPv4 and IPv6.
ESP may be applied alone, in combination with AH, or in a nested fashion.
ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.

The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.
Using encryption-only for confidentiality is allowed by ESP but not recommended.
This will provide defense only against passive attackers. Using encryption without a strong integrity mechanism on top of it (either in ESP or separately via AH) may render the confidentiality service insecure against some forms of active attacks.

NOTE: Data origin authentication and connectionless integrity are joint services, referred to jointly as "integrity".

On a per-packet basis, the computation being performed provides connectionless integrity directly; data origin authentication is provided indirectly because of binding the key used to verify the integrity to the identity of the IPsec peer. Typically, this binding is effected through the use of a shared, symmetric key.

Internet Security Association and Key Management Protocol (ISAKMP) - provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records.

**Transport mode** - only the payload (ESP) of the IP packet is usually encrypted or authenticated.

- The AH part of IPSec is integrity and authentication and ESP is confidentiality.
- The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be modified by network address translation(NAT), as this always invalidates the hash value. The transport and application layers are always secured by a hash, so they cannot be modified in any way, for example, by translating the port numbers.

NOTE: A means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

**Tunnel mode** - the entire IP packet (AH & ESP) is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.

- Most secure mode for IPSec.
- Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).
- Tunnel mode supports NAT traversal.

**IaaS** – Object and Volume storage.

**PaaS** - Structured and Unstructured. Structured would be database like and searchable. Unstructured would be text, multimedia, email, etc.

**SaaS** – Data entered via web interface. The two most common storage types for SaaS are information storage and management as well as content and file storage within the application.
- Information Storage and Management: Data entered in system via web UI are stored in SaaS (DATABASE).

Cloud environment will typically use RAID and SAN storage systems that are connected physically to the underlying infrastructure.
Object storage is typically flat and uses HTTP and file storage. FS is hierarchical. “Flat object”
Object Storage for IaaS needs synchronization across all the data. Requires APIs for retrieval.
Object storage contains metadata that allows easy access from the web.

For **Object storage**:

- Encryption at the actual file level handled by the cloud provider
- Encryption can be used within the application itself through IRM technologies or via encryption within the application itself.

With **application-level encryption**, the application effectively acts as a proxy between the user and the object storage and ensures encryption during the transaction. However, once the object has left the application framework, no protection is provided.

**Content Delivery Network (CDN)** – Stored in object storage then distributed geographically. Multimedia streaming services. Rather than dragging data from a datacenter to users at variable distances across a continent, the streaming service provider can place copies of the most requested media near metropolitan areas where those requests are likely to be made.

Volume can be associated with block or raw storage.

- Block is associated with a SAN, RAID, and iSCSI.
- Challenges of block storage include: Requires greater administration and may require OS or application to store, sort, and retrieve data.

Use case for block storage include: Data of multiple types and kinds, such as enterprise backup services.

For **volume storage**:

Many of the typical encryption systems used on a traditional server model can be employed within a cloud framework.

The most prevalent communications protocol for network-based storage is iSCSI, which allows for the transmission and use of SCSI commands and features over a TCP-based network. Whereas a traditional data center will have SAN (storage area network) setups with dedicated fiber channels, cables, and switches, in a cloud data center this is not possible with the use of virtualized hosts. In this case, iSCSI allows systems to use block-level storage that looks and behaves like a SAN would with physical servers, but it leverages the TCP network within a virtualized environment and cloud.

iSCSI also supports a variety of authentication protocols, such as Kerberos and CHAP, for securing communications and confidentiality within networks. iSCSI is not encrypted by itself and must be protected by other means.

**Converged Networking Model** – Optimized for cloud deployments and underlying storage.

- Maximizes benefits of a cloud workload

In SaaS, the 2 delivery modes (licensing) of S/W to customer are

- via the cloud (hosted application management) or
- provide customer access to the provider's proprietary S/W (S/W on demand)

Encryption system Architecture has three basic components:

- the data itself,
- the encryption engine that handles all the encryption activities, and
- the encryption keys used in the actual encryption

Encryption should be used wherever possible to protect communications between virtual machines and storage networks.

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

- Manages the use, performance and delivery of cloud services.
- Negotiates relationships between cloud providers and cloud consumers.

**Logical Design** –Part of the Design phase in SDLC.

- Lacks specific details such as technologies and standards with general focus. Communicates abstract concepts such as routers and switches without detail.
- It lacks technology detail and standards
- It communicates with abstract concepts (network, routers, system)

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

- To show the hardware used to deliver the system
- Created from logical design
- Expands element from logical design

**Shibboleth** – Usually associated with academic institutions.

Best way to protect an **RDP** session is with a **SMART CARD**.

**CSRF** – Think cookies

**XXS** – Invalid input from untrusted data

**Encoding** is a process used to prevent the introduction of malicious characters into a web application.

**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 – provides privacy/security, and integrity. Is successor to SSL.

The **TLS handshake protocol** negotiates and establishes the connection.

- Negotiates encryption algorithm and keys before data is sent or received.
    - Cipher suite negotiation
    - Authentication of the server
- Client Session key information exchange
- Negotiates and establishes the TLS connection between two parties.
- It also handles the key exchange and establishes the session ID.
- It does not perform the actual encryption of data packets.

The **TLS record protocol** is the actual secure communications method for transmitting data;

- TLS performs the authentication and encryption of data packets, and in some cases compression as well. Handles the secure communication and transit of data.
- It is responsible for the encryption and authentication of packets throughout their transmission between the parties
- In some cases it also performs compression.
- Ensure connection is private and reliable.
- It is also leveraged to verify integrity and origin of the application data.

**Rapid elasticity** vs **Rapid scalability** – RE allows cloud customers to allocate resources as needed for immediate usage and RS is ability of cloud to quickly meet demand.

**Vertical cloud computing** refers to the idea of creating and managing a specific cloud and cloud services to appeal to a specific industry.

The **Apache CloudStack** was a specifically designed open source cloud computing IaaS platform developed to help IaaS provide a complete "stack" of features and components for cloud environments.

**Resource pooling** – Allows access to resources as needed.

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

- Level 1 - There are no physical security requirements at Level 1. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.
- Level 2 - Requires role-based authentication where a cryptographic module is used for actual authentication processes. 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. The module must also have mechanisms that show evidence of any attempts to tamper with it
- Level 3 - Requires physical protection methods to ensure a high degree of confidence that any attempts to tamper are evident and detectable. It requires the cryptographic module to not only authenticate the user to the system but also to verify authorization. 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 covers/doors are removed.

- 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.

All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing may select any of the twenty-two accredited labs.

**Data Centers Design Standards**

The guidelines from America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) establish:

- 64.4 - 80.6 degF (18-27degC) as the optimal temperature for a data center. Thermostat on return air may result in high energy costs
- Humidity (Dew point range: 41.9 - 50.0 degF), 40-60 % relative humidity as optimal for a data center. Too low increases static, too high increases corrosion and bio creep.
- HVAC: The hot aisle/cool aisle approach (hot air output face each other, cool air face away) makes cooling data centers more efficient. Pump cool air into the cool aisle and extract hot air from hot aisle.

Building Industry Consulting Services International (BICSI) issues certification for data center cabling & design Installation.

The standards put out by BICSI primarily cover complex cabling designs and setups for data centers, but also include specifications on power, energy efficiency, and hot/cold aisle setups.

The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Data center location, facility structure, infrastructure and application

The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities.  Requirement for temperature, emergency.

The Uptime Institute publishes the most commonly used and widely known standard on data center tiers and topologies.

- Tier 1 is Basic Data Center Structure. Has a single path for power and cooling and few, if any, redundant and backup components. It has an expected uptime of 99.671% (28.8 hours of downtime annually).
- Tier 2 is Redundant Site Infrastructure. Redundant components but only one path/source or partial redundancy in data center
- Tier 3 is Concurrently maintainable. A Tier III data center is concurrently maintainable with redundant components as a key differentiator, with redundant distribution paths to serve the critical environment.99.982% Guaranteed availability.
- Tier 4 is Fault-tolerant and zero single points of failure. Several independent and physically isolated systems that act as redundant capacity components and distribution paths. 99.995 % uptime.

**UPS** – Should last long enough for a graceful shutdown.
UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations.

A **generator** transfer switch should bring backup power online before the UPS duration is exceeded.
UPS – Last long enough for graceful shutdown.
Generator fuel to last 12 hours is recommended

**Hot aisle containment** -  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

**Chicken coop datacenter** – Long side facing the prevailing wind to allow for natural cooling.
Raised floors need to be 24 inches.
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

- Tightly Coupled: Both nodes work together to increase performance. Has a set max capacity. A tightly coupled cluster should see improved performance as more drives and nodes are added to the environment.
- Loosely Coupled: Loosely coupled clusters have the downside that maximum performance and capacity is limited to the performance of the node that houses the data. The performance does not scale up as nodes are added like a tightly coupled cluster does.
- As a result loosely coupled clusters tend to be applied where performance is important but inexpensive capacity is more important.

**CSA** or cloud service agreement 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.

**UC** - Underpinning contracts – External contracts between organizations and vendors or suppliers.

**Release** and **Deployment management** needs to be tied to change management, config management, and problem management. With Release Management think of software and releasing versions.

**Change management** involves the creation of an RFC ticket and obtaining approval.

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

**Verification** and **validation** should occur at each stage of the SDLC. User input is considered in define phase. Software construction is related to the design phase.

**Puppet** and **Chef** can help during the secure operations phase.

Two very popular tools for maintaining system configurations and versioning of software are Puppet and Chef.

- Puppet is a commonly used tool for maintaining system configurations based on policies, and done so from a centralized authority. Configuration management system, you define the state of IT infrastructure and Puppet then enforces the correct state
- Chef — you automate how you build, deploy, and manage architecture. Chef server stores "recipes". Chef client is installed on each node, periodically polls the Chef server for the latest policy.
- Ansible — software provisioning, application deployment, and configuration management

**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 Architecture**

DLP – Uses media-present checks for IP data.

**Data in Motion**

- Network based or gateway DLP - the engine is deployed near the org gateway to monitor outgoing protocols like HTTP, HTTPS, FTP and SMTP.

Data at Rest: Looks for data loss on storage.

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

**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.

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

Enterprise risk management are the processes and structures used in systematically managing all enterprise risks.

**Restatement of Law** - Uses relevant factors of applicable law. Articulate the principles or rules for a specific area of law. Judges use these restatements to assist them in determining which laws should apply when conflicts occur.

**Doctrine of Proper Law** – Addresses jurisdictional disputes. When there are more than one law involved in a case, and a superior law needs to be determined. Think proper jurisdiction.

**Applicable Law** - This determines the legal standing of a case or issue.

**Plain View Doctrine** - Exception to the Fourth Amendment's warrant requirement that allows an officer to seize evidence and contraband that are found in plain view during a lawful observation.

**Common Law** - The existing set of rulings and decisions made by courts, informed by cultural motives and legislation. These create precedents, which each party will cite in court as a means to sway the court to their own side of a case.

**Tort Law** - Refers to the body of rights, obligations, and remedies that set out reliefs for persons who have been harmed as a result of wrongful acts by others. Tort actions are not dependent on an agreement between the parties to a lawsuit.

**Prudent Person Rule** - Based on a judge's discretion, can demonstrate a party acted responsibly as a prudent person would.

**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**

- Damage – how bad would an attack be?
- Reproducibility – how easy is it to reproduce the attack?
- Exploitability – how much work is it to launch the attack?
- Affected users – how many people will be impacted?
- Discoverability – how easy is it to discover the threat?

**Logs for API calls** may also carry with them regulatory requirements for both the level of log detail and the required retention periods.

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

Data Center traffic - More specifically, northbound interfaces go towards the core of the data center or towards the Internet-facing egress of the network. Southbound goes towards the end-users/servers/VMs.

East-West Traffic denotes a direction of traffic flow within a data center.

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

- DNSSEC relies on digital signatures and allows a client lookup to validate a DNS record back to its authoritative source, a process known as zone signing.
- The integration of DNSSEC and the validation that it performs do not require any additional queries to be performed.

**DNSSEC**: Protects against DNS poisoning

**Threats to DNS infrastructure**:

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

**X500** – LDAP (Lightweight directory access protocol)

**Digital Signatures** – Use sender's private key plus a hash to guarantee integrity and origin. PKI

**X509** is a standard defining the format of public key certificates.

- X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.
- Contains a public key and an identity (a hostname, or an organization, or an individual).

**Certificate pinning** is a method of associating X.509 certificate and its public key to a specific CA or root.

Typically, certificates are validated by checking a verifiable chain of trust back to a trusted root certificate.

Certificate pinning bypasses this validation process and allows the user to trust "this certificate only" or "trust only certificates signed by this certificate."

Authoritative Source - The "root" source of an identity, such as the directory server that manages employee identities.

What risk does certificate pinning mitigate? malicious root cert or rogue CA

**Trusted Platform Module (TPM)** – Full disk encryption capability. Integrity and authentication to boot process. Has unique RSA key burned into it. Cloud-based software applications can use a 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 performs tasks as a crypto processor.

**Hardware Security Module (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.

HSM is a removable or external device that can generate, store, and manage RSA keys used in asymmetric encryption. HSMs are used with high-volume e-commerce sites to increase the performance of SSL sessions.

A HSM is a physical computing device that provides crypto processing and safeguards and manages digital keys for strong authentication.

The key difference between HSM and TPM is that an HSM manages keys for several devices, whereas a TPM is specific to a single device.

**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 on 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 – Software, Data, Keys

WORM - Write once read many (WORM) describes a data storage device in which information, once written, cannot be modified. Is considered long term.

UPS – Needs to last long enough for graceful shutdown

Generator should last 12 hours.

Portability – Enables the migration of cloud services from one cloud provider to another or between a public cloud and a private cloud.

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.

Authentication – Identifies individual and ensures who he/she is

Authorization – What access does the individual have

Cloud directory services use protocols like LDAP ( X500) and SAML to link user identities to cloud applications.

SAML 2.0 is an OASIS standard for federated identity management that supports both authentication and authorization.

- Uses XML to make assertions between an identity provider and a relying party.
- Assertions can contain authentication statements, attribute statements, and authorization decision statements

Security Tokens

- Simple Web Tokens
- JSON Web Tokens (JWT)
- SAML assertions

SSO – Think within an enterprise. Allows a user to access multiple apps with a single set of credentials.

- Multiple applications over a single set of credentials in an enterprise.

Federated SSO – Think outside the enterprise. 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 is usually within an organization.

Federated SSO is between organizations.

- Federation always includes SSO.
- SSO doesn't always need federation.

**SAML 2.0**

Standard for federated identity management that supports both authentication and authorization.

- Uses XML to make assertions between an identity provider and a relying party.
- Assertions can contain authentication statements, attribute statements, and authorization decision statements.
- SAML is very widely supported by both enterprise tools and cloud providers but can be complex to initially configure
- Allows business to make assertions on identity, attributes, and entitlements.
- Parts of SAML are attributes, bindings, protocols, profiles.

In a federated system, SAML sends a SAML assertion to the service provider (relying party)containing all the information that the service provider requires to determine the identity, level of access warranted, or any other information or attributes about the entity.

- Identity provider resides at the user's home organization and performs authentication and then passes it to a relying party to grant access. Think of them as the ones providing the identity.
- Relying party - Entity that takes the authentication tokens from an identity provider and grants access to resources in federation. The relying party is usually the service provider and consumes these tokens.

In a Trusted 3rd-party model of federation, each member organization outsources the review and approval task to a third party (proxy) they all trust. This makes the third party the identifier (Identity provider) (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

Cross-certification – Each group vet and approves each other. Also called web of trust.

WS-Federation – "Defines mechanism to allow different security realms to federate such as authorized access to resources" , used by Active Directory Federation Services (ADFS). Relies on SOAP.

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.

OAuth is an IETF standard for authorization that is very widely used for web services (including consumer services).

- OAuth is designed to work over HTTP and is currently on version 2.0, which is not compatible with version 1.0.
- Allows API authorization between apps. "Enables 3rd party application to obtain limited access to an HTTP service" either on behalf of resource owner, or by allowing 3rd parties to obtain access on own behalf.
- Allows 3rd party app to retrieve user data without user needing to share login credentials.
- It is most often used for delegating access control/authorizations between services.

OAuth 2.0 is more of a framework and less rigid than OAuth 1.0, which means implementations may not be compatible. It is most often used for delegating access control/authorizations between services

OpenID is a standard for federated authentication that is very widely supported for web services.

- It is based on HTTP with URLs used to identify the identity provider and the user/ identity.
- The current version is OpenID Connect 1.0 and it is very commonly seen in consumer services.
- Allows users to authenticate across websites or apps ….. provides authentication but not authorization.
- Let's developers authenticate their users across websites and apps.
- Developers can leverage OpenID as an open and free authentication mechanism and tie it into their code and applications, without being dependent on a proprietary or inflexible system.
- It relies on REST and JSON.

There are two other standards that aren't as commonly encountered but can be useful for cloud computing:

- eXtensible Access Control Markup Language (XACML) is a standard for defining attribute-based access controls/authorizations. It is a policy language for defining access controls at a Policy Decision Point and then passing them to a Policy Enforcement Point. It can be used with both SAML and OAuth since it solves a different part of the problem—i.e. deciding what an entity is allowed to do with a set of attributes, as opposed to handling logins or delegation of authority.
- System for Cross-domain Identity Management (SCIM) is a standard for exchanging identity information between domains. It can be used for provisioning and deprovisioning accounts in external systems and for exchanging attribute information.

Proxy federation could use a 3rd party to optimize compliance with security governance. A federation server proxy collects credentials or home realm details from Internet client computers by using the logon, logout, and identity provider discovery. 3rd party for identification federation=proxy

Proxy - A forward proxy is the intermediary that the client puts forward between itself and any server.

The reverse proxy is at the other end – something the server puts forward between itself and any client. In short, a reverse proxy is an intermediary on the side of the server you are connecting to. And the forward proxy is the intermediary on your side of the internet.

Cloud providers IAM system

HTTP request signing is very commonly used for authenticating REST APIs and authorization decisions are managed by internal policies on the cloud provider side.

- The request signing might still support SSO through SAML, or
- the API might be completely OAuth-based, or
- use its own token mechanism.

The cloud provider is responsible for enforcing authorizations and access controls.

The cloud user is responsible for defining entitlements and properly configuring them within the cloud platform.

Cloud platforms tend to have greater support for the Attribute-Based Access Control (ABAC) model for IAM, which offers greater flexibility and security than the Role-Based Access Control (RBAC) model.

RBAC is the traditional model for enforcing authorizations and relies on what is often a single attribute (a defined role).

ABAC allows more granular and context aware decisions by incorporating multiple attributes, such as role, location, authentication method, and more. ABAC is the preferred model for cloud-based access management.

When using federation, the cloud user is responsible for mapping attributes, including roles and groups, to the cloud provider and ensuring that these are properly communicated during authentication. These should be based on an authoritative source.

Cloud providers are responsible for supporting granular attributes and authorizations to enable ABAC and effective security for cloud users.

Cloud users should prefer MFA for all external cloud accounts and send MFA status as an attribute when using federated authentication.

Privileged identities should always use MFA.

Account and session recoding should be implemented to drive up accountability and visibility for privileged users.

Develop an entitlement matrix for each cloud provider and project, with an emphasis on access to the metastructure and/or management plane.

Translate entitlement matrices into technical policies when supported by the cloud provider or platform.

CSP is responsible for the hypervisor.

**API gateway** is a device that filters API traffic and can either be a proxy or a specified part of your application stack that comes into play before data is processed.

It can also implement access controls, rate limiting, logging, metrics, and security filtering.

**XML gateway** (H/W or S/W - based) transforms how services and sensitive data are exposed as APIs to developers, mobile users, and the cloud.

- Can provide AV and DLP security controls.
- Can be a reverse proxy and perform content (XML, SFTP) inspection.
- Popularly implemented in service-oriented architectures to control XML-based web services traffic, and increasingly in cloud-oriented computing to help enterprises integrate on-premises applications with off-premises cloud-hosted applications.

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

**Web Application Firewalls (WAF)** – (Layer 7) WAF filters HTTP traffic and can prevent DOS attacks.

**Database Activity Monitoring (DAM**) - Host-based or network-based - (Layer 7) Prevents malicious code (SQL based attacks) from executing. Monitor all requests made to a database, particularly those made by administrative users, and then watch for signs of suspicious activity, flagging it for review or direct intervention.

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

Asymmetrically sends symmetric key

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.

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

Containers provide you with a standard way to package your application's code and dependencies into a single object. You can also use containers for processes and workflows in which there are essential requirements for security, reliability, and scalability.

Application virtualization is a software implementation that allows applications and programs to run in an isolated environment rather than directly interacting with the operating system. (No OS involvement)

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

- Storage controller is a device that orchestrates access to and allotment of resources.
- Storage controllers will be used in conjunction with iSCSI, fibre channel, fibre channel over ethernet,

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 measured in time

MTD – Focused on point in time after the outage

Certification -> Accreditation - and then operation

Certification is used for verifying that personnel have adequate creds to practice certain disciplines.

Accreditation is the formal declaration by a neutral third party that the certification program is administered in a way that meets the relevant norms or standards of certification program (e.g., ISO/IEC 17024).

Certification bodies are getting accredited, while companies are getting certified. (The certification body needs to be compliant with the standard ISO 17021 if they want to get accredited for certifying management systems.)

General server security – 800-123

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.

- A problem is the unknown cause of one or more incidents, often identified as a result of multiple similar results.
- A known error is an identified root cause of a problem.
- A workaround is a temporary way of overcoming technical difficulties.

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

Securing the Hypervisor involves the following:

- Install all updates to the hypervisor as they are released by the vendor. Centralized patch management solutions can also be used to administer updates.
- Restrict administrative access to the management interfaces of the hypervisor.
- Protect all management communication channels using a dedicated management network.
- Disconnect unused physical hardware from the host system.

- Disable all hypervisor services such as clipboard - or file-sharing between the guest OS and the host OS unless they are needed.
- Consider using introspection capabilities to monitor the security of each guest OS and their interactions.

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 --> report --> classify --> investigate --> collect data --> resolution with approval and then ==> implement changes

Utility is functionality of product.

Warranty is assurance the product will meet requirements.

Application Security Management Process (ASMP):

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

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

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.

ISO / IEC 27034 -1 defines ASMP to manage and maintain each ANF.

1. Specifying the application requirements and environment
2. Assessing application security risks
3. Creating and maintaining the ANF
4. Provisioning and operating the application
5. Auditing the security (SAC PA) of the application

Software Testing:

Validation: Ensures software meets requirements. “Are we building the right software?” Validate Requirements

Verification: Ensures software functions correctly. “Are we building the software right?” Verify Software

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

Fuzzing - Automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

Vulnerability scans depend on vulnerability signatures

Mobile number is considered PII in EU but not US

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

Synthetic performance monitoring better than real time user monitoring because it is more comprehensive but it is not real time.

- Synthetic agents can simulate user activity in a much faster manner than real-user monitoring and perform these actions without rest.

    Synthetic performance monitoring approximates user activity and thus, is not as accurate as RUM.

Static Application Security Testing (SAST):

- White box testing. Test code. Done without executing the application.
- Determines coding errors. Early development life cycle.
- Useful for XSS, SQL Injection, Backdoors.
- Generally considered white box test. Inspects the code and can help against XSS, SQL injection, and buffer overflows.

Dynamic Application Security Testing (DAST):

- Black box testing. Done at the runtime.
- Useful to test exposed HTTP and HTML Interfaces.
- Considered black box. Looks at execution paths and in a running state. Web vulnerability testing and fuzzing are considered DAST tests.

Runtime Application Self Protection (RASP):

- Considered to focus on application that possesses self-protection capabilities.
    - Prevents attacks by self-protecting without human intervention.
    - Focuses on apps that that have self-protection capabilities in runtime environments. Works without human intervention in response to attacks.

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. LAN tech.

- iSCSI is 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.
- iSCSI is unencrypted - Encryption must be added separately through IPsec (tunneling) and IKE (security).

HIDS monitors network traffic as well as critical system files and configurations.

After the accreditation of a system by the designated approving authority (DAA), an authorization to operate (ATO) is granted for 3 years.

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.

SDLC Define (requirements documented), Design (user stories), Develop (code written), Test (pen tests and vuln assessments), Secure ops, Disposal.

The 3 types of security trainings are initial, recurring and refresher.

SETA - Awareness is for all employees, while training is for specific employee based on need.

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 (Non-mission critical) + Private (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

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

**IaaS**

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

**SaaS**

| **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. Focuses on IRM and DRM solution

Difference between end to end vs link encryption for data in transit?

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.

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).

Object storage can use the following types of encryption:

○ File-level encryption IRM/DRM allows creator of file to embed permissions based on attributes. These restrictions protect the file regardless of 3rd party assets. The encryption engine is commonly implemented at the client side (in the form of an agent) and preserves the format of the original file.

○ Application-level encryption. The encryption engine resides in the application that is using the object storage, or can be implemented on a customer gateway/proxy. This type of encryption can be used with: Database encryption, Object storage encryption, and proxy encryption. Not good for searching, indexing DB.

Client-side encryption: When object storage is used as the back-end for an application (including mobile applications), encrypt the data using an encryption engine embedded in the application or client.

Database Encryption can use file or application-level encryption. Also, most DBMS can provide transparent encryption that is seamless to the user, with the engine residing within the database.

- 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 3rd party:

Trusted 3rd party provides key escrow services. It's important to evaluate the security of 3rd party storage.

Key distribution

Keys should never be distributed in the clear. Often, passing keys out of band is a preferable, yet cumbersome and expensive, solution.

Note: Always Encrypt data prior to its arrival to cloud environment.

Encryption Best Practices

- Use open and validated formats (Algorithms should be strong and publicly known)
- All encryption keys should be stored within the enterprise, as opposed to with CSP. Keying material should never be stored on same volume as encrypted data
- Identity-based key assignment and protection of private keys
- Use strong encryption
- Follow key management best practices for location of keys
- SoD would require that key management functions should be conducted separately from the cloud provider

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.

Data rights management (DRM) is an extension of normal data protection, where additional controls and ACLs are placed onto data sets that require additional permissions or conditions to access and use beyond just simple and traditional security controls. This is encapsulated within the concept of information rights management (IRM).

DRM applies to the protection of consumer media, such as music, publications, video, movies, and so on. In this context, IRM applies to the organizational side to protect information and privacy, whereas DRM applies to the distribution side to protect intellectual property rights and control the extent of distribution.

DRM mechanisms

- Rudimentary Reference Check
- Online Reference Check
- Local Agent Check
- Presence of Licensed Media
- Support-Based Licensing

DRM Provides

- Persistent Protection
- Dynamic Policy Control
- Automatic Expiration
- Continuous Auditing
- Replication Restrictions
- Remote Rights Revocation
- Might provide more

IRM Challenges

- IRM requires that all users with access should have matching encryption keys. This requires a strong and comprehensive identity structure.
- Each user will need to be provisioned with an access policy and keys
- Access can be identity based or role based (RBAC)
- Access can be implemented with a single director location or across federated trust
- End users will likely have to install a local IRM agent for key storage or authenticating and retrieval of protected information
- Can be challenging with disparate systems and document readers

IRM and DRM solutions are File level type of encryption

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

SIEM can help prevent escalation of privilege

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.

Problem management is focused on identifying and mitigating known problems and deficiencies before they occur.

Continuity management (BCM) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster.

BCM is 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.

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.

Business Continuity efforts - maintaining critical operations during an interruption in service

An event is an unscheduled adverse impact to operations. An event is distinguished from a disaster by its duration

BIA lists assets (criticality, value, etc), input for BC/DR

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.

Disaster Recovery efforts - resuming operations after an interruption due to disaster

BCDR Steps: Define, Analyze, Assess Risk, Design, Implement, Test. DAAD IT

BCDR Plan

- A list of items from the Asset Inventory deemed critical
- The circumstances under which an Event or Disaster is declared
- Who is authorized to make the declaration
- Essential point of Contact
- Detailed Actions, Tasks and Activities

BCDR Plan - Notes

- Authorized party also declares cessation of BCDR activities
- This should only be done once there is a high degree of confidence that all safety and health hazards are cleared, operations is back to normal
- Doing this too soon can exacerbate the disaster or create a new one

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.
Resiliency - The ability to restore normal operations after a disruptive event. Redundancy is the foundation of resiliency.
Urban Design for data centers – Municipal codes can restrict building design.

**Testing BCDR**

**Table-top** - structured walkthrough
**Walk-through test** – Also called a simulation test is more involved than a table-top. Simulates a disaster but only includes operations and support personnel.
**Functional Drill** – Also called a parallel test, it involves moving personnel to recovery site. All employees are involved here.
**Full interruption** – Most involved and include moving key services and transactions to backup and recovery sites. Close to real life scenario.

**3 Ps** – **Power**, **Pipe**, and **Ping** - The ping means that computers are accessed remotely; the power is the electricity, and the pipe is the connection to the Internet.

**Forklifting** – Moving everything to the cloud. Large migration.

Data security and GRC are always customer responsibility.

**Federation Standard**

SSO is the ability to authenticate a single time and gain access to multiple systems in the enterprise.

SSO prevents users from having to memorize multiple authentication factors for different systems., but SSO in itself does not provide API authorization between applications.

**SAML** — the most commonly used federation. XML-based framework to communicate user authentication, authorization, and attributes. Authentication tokens are digitally signed XML, moved over TLS.

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

SAML is an XML framework for communicating user authentication, entitlement, and attribute information. It is not used for API authorization.

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

Entitlement maps identities to authorizations and any required attributes (e.g. user x is allowed access to resource y when z attributes have designated values). We commonly refer to a map of these entitlements as an entitlement matrix.

WS-Federation: federation within the broader WS-Security or WS-* framework.

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.

WS-Federation can be used directly by SOAP applications and web services. WS-Fed is a protocol that can be used to negotiate the issuance of a token. You can use this protocol for your applications (such as a Windows Identity Foundation-based app) and for identity providers (such as Active Directory Federation Services (ADFS) or Azure AppFabric Access Control Service).

**Open ID Connect**: based on OAuth, lower security.

Interoperable authentication protocol based on OAuth 2.0.

OpenID connect is an authentication mechanism based on Oauth that allows users to authenticate across websites or applications. It provides authentication, not authorization

OpenID connect is a federation protocol that uses REST/JSON. It was specifically designed with mobile apps in mind instead of only web-based federation.

OAuth: Used for authorization (OAuth 2.0) Not Designed for SSO.

widely used for web and mobile access. Users can grant websites or applications access to their information on websites, without giving them the passwords.

Oauth allows API authorization between applications. It allows 3rd party application to retrieve a user's data without the end User needing to share login credentials.

Shibboleth Standard: based on SAML, open & free. User authenticates with their organization's credentials and the organization (Identity Provider) passes information to service providers.  Usually used by Universities.

XACML — eXtensible Access Control Markup Language. It's an Attribute-Based Access Control system. Attributes associated with a user or action or resource are inputs to the access-control decision.

All of these technologies are part of federated identity management that allows users to be authenticated across enterprise boundaries, meaning that a user logs into his local domain and gain access to resources in other enterprise based on trust relationships.

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. Has a set max capacity. A tightly coupled cluster should see improved performance as more drives and nodes are added to the environment. Delivers a high-performance interconnect between servers. Allows for load-balanced performance. Allows for maximum scalability as the cluster grows (array controllers, I/O ports, and capacity can be added into the cluster as required to service the load). Fast, but loses flexibility*

- **Loosely Coupled**:

Loosely coupled clusters have the downside that maximum performance and capacity is limited to the performance of the node that houses the data. The performance does not scale up as nodes are added like a tightly coupled cluster does. As a result, loosely coupled clusters tend to be applied where performance is important but inexpensive capacity is more important. This allows performance to scale with capacity. Scalability is limited by the performance of the interconnect.

Loose Coupling for cloud resources is by far the most desired paradigm for RESTful API development. RESTful APIs should be able to transform, remix, scale, extend and morph from use case to use case across multiple resources.

- HA is loosely coupled and Fault tolerant is tightly coupled

**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

Air gapped push buttons – KVMs and physically break a connection before a new one is made.

- Air-gapped pushbutton on KVM switches physically break the current connection before a new one is made.
- Tamper labels are used to alert you that someone has physically accessed the system and torn the labels. They are applied to cases of devices that you need to remain secure. While they do not prevent physical access, they alert if the physical access has occurred.
- Fixed firmware is device software that cannot be erased or altered. Fixed firmware is installed on internal chips in the device.
- Secure data ports reduce the likelihood of data leaking between computers that are connected through the KVM by protecting the ports.

Using cloud storage is considered “processing” by most frameworks and laws.

There are three different types of SAML Assertions – authentication, attribute, and authorization decision.

- **Authentication assertions** prove identification of the user and provide the time the user logged in and what method of authentication they used (I.e., Kerberos, 2 factor, etc.)
- The **attribution assertion** passes the SAML attributes to the service provider – SAML attributes are specific pieces of data that provide information about the user.

- An **authorization decision assertion** says if the user is authorized to use the service or if the identify provider denied their request due to a password failure or lack of rights to the service.

Assertions can contain authentication statements, attribute statements, and authorization decision statements.

Kerberos is a network authentication protocol that uses secret-key (symmetric) cryptography.

Reads and writes being slow on the cloud – **disk related**.

Level 2 STAR Assessment – 3rd party review against SOC2 SOC 2 Attestation
Level 2 STAR Certification - 3rd party review against ISO ISO Cert
Level 2 C-Star – Chinese Standards

**Cloud Certification Schemes List (CCSL)** provides an overview of different existing certification schemes.

**Risk Treatment**

- Accept the risk = Cost of opportunity is higher over risk.
- Transfer the risk = Financial burden transfer, still risk own by customer.
- Avoid the risk = Business Decision.
- Mitigate risk = Implement countermeasure to reduce to an acceptable level.

**Remote Key Management Service** – A remote key management service is maintained and controlled by the customer at their own location. This offers the highest degree of security for the consumer.

**Client-Side Key Management Service** – Most common with SaaS implementations, client-side KMS is provided by the cloud provider but is hosted and controlled by the consumer. This allows for seamless integration with the cloud environment. But also allows complete control to still reside with the consumer. Client-Side Key Management is PROVIDED by the provider for you to use, and mainly used with SaaS solutions, versus providing the Remote Key management yourself, which is a higher degree of security. But it is important to note both reside on your own premises.

**Virtual Switches Secure Configuration**:

- Physical NIC redundancy to redundant physical switches
- Port channeling

**Network isolation** (management plane vs. virtual switches vs. VM traffic)

Internal and external network isolation

Use security applications that are virtual network aware (IPS, etc.)

Vertical cloud computing A vertical cloud, or vertical cloud computing, describes the optimization of cloud computing and cloud services for a vertical (i.e., a specific industry) or specific use application.

**Virtual Extensible LAN (VXLAN)** Encapsulates layer 2 frames within layer 4 UDP packets, using some techniques like VLAN but supporting up to 16 million logical networks.

**Virtual Private Cloud (VPC)** A logically isolated section of a cloud (not a private cloud per se) where resources can be launched in a virtual network that is customer defined. The customer has complete control over their virtual networking environment, including selection of private IP address range, creation of subnets, and configuration of route tables and network gateways.

**Virtual Machine Introspection (VMI)**

Allows for agentless retrieval of the guest OS stage, such as the list of running processes, active network connections, and opening files.
An agentless means of ensuring a VM's security baseline does not change over time. It examines such things as physical location, network settings, and installed OS to ensure that the baseline has not been inadvertently or maliciously altered.
Used for malware analysis, memory forensics, and process monitoring and for externally monitoring the runtime state of a virtual machine.
The introspection can be initiated in a separate virtual machine, within the hypervisor, or within another part of the virtualization architecture.
The runtime state can include processor registers, memory, disk, network, and other hardware-level events.

**Agile Characteristics:**

- Often involves daily meetings called Scrums
- Favors customer collaboration and prototyping instead of an elaborate contract mechanism.
- Works in short, iterative work periods (between a week and month in duration).
- Prototyping is favored over testing
- Relies on cooperative development instead of expertise
- Does not depend on planning.

**PCI DSS Payment Card Industry Data Security Standard**

PCI DSS is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI-SSC). The standard was created to increase controls around cardholder data to reduce credit card fraud.

It is a comprehensive and intensive security standard that lists both technical and nontechnical requirements based on the number of credit card transactions for the applicable entities.

Validation of compliance is performed annually or quarterly, either by

- an external Qualified Security Assessor (QSA) or by a firm-specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or
- by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

**PCI-DSS Compliance levels**

Level 1 – Over 6 million transactions annually
Level 2 – Between 1 and 6 million transactions annually
Level 3 – Between 20,000 and 1 million transactions annually
Level 4 – Less than 20,000 transactions annually

PCI DSS stresses that organizations either upgrade or disable any fallback to SSL/early TLS.(TLS 1.1 or SSL 3.0)

If they have not already, companies in transition should have a formal Risk Mitigation (POAM) and have a Migration Plan in place as well.

Each card issuer maintains their own table of compliance levels.

The 6 goals are broken down to 12 requirements:

12 requirements list more than 200 controls.

**PCI-DSS Security Objectives**:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

Each requirement/sub-requirement is additionally elaborated into three sections.

- Requirement Declaration
- Testing Processes
- Guidance

**PCI-DSS Requirements**

1. Installing and maintaining a firewall configuration to protect cardholder data
2. Changing vendor-supplied defaults for system passwords and other security parameters
3. Protecting stored cardholder data
4. Encrypting transmission of cardholder data over open, public networks
5. Protecting all systems against malware and performing regular updates of anti-virus software
6. Developing and maintaining secure systems and applications
7. Restricting access to cardholder data to only authorized personnel
8. Identifying and authenticating access to system components
9. Restricting physical access to cardholder data
10. Tracking and monitoring all access to cardholder data and network resources
11. Testing security systems and processes regularly
12. Maintaining an information security policy for all personnel