CCSP – Certified Cloud Security Professional

A Quick Recap! Important Concepts. Last minute review before Exam

By:

Muhammad Ahmad

Agenda & Objective

- Quick recap of important topics
- Overview of all domains' key concepts
- Getting ready to Pass the CCSP exam

References & Credits

- *(ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, 2nd Edition*
- *CCSP Certified Cloud Security Professional All-in-One Exam Guide Book by Daniel Carter*
- *CCSP For Dummies by Arthur J. Deane*
- *CCSP Official (ISC)2 Practice Tests by Ben Malisow*
- *Mike Chapple CCSP Notes*
- *Multiple topics search over google*
- *Images used in the presentation may be copyrighted to their respective owners, taken from google for better visual presentation.*

About Me!

A seasoned professional with ~15 years of experience in Commercial & Microfinance Banks/Financial Institutes, MNCs, and ISP. Beside academic qualifications (MS in Computer Science, MBA, B.Sc.(Hons) in Computer Science), my professional qualification includes International certifications & trainings of CISSP, CCSP, CRISC, CISA, CISM, CGEIT, ISMS LA ISO27001, ISO27005 SLRM, and ITIL. I am also a regular trainer for CISSP, CCSP, CISA, CISM, CGEIT, CRISC, and ITIL. I have experience in:

- *Information/Cyber Security Management*
- *IT Governance & Management*
- *Risk and Compliance Management*
- *IS Audit & Controls*
- *IT Services Management*
- *Business Solutions & IT Operations*
- *Strategic Outsourcing & Data Center*
- *Business Continuity & DR Management*
- *Project Management*

Contact Me

Email: mahmad83@gmail.com

Cloud Concepts, Architecture and Design

Domain 1

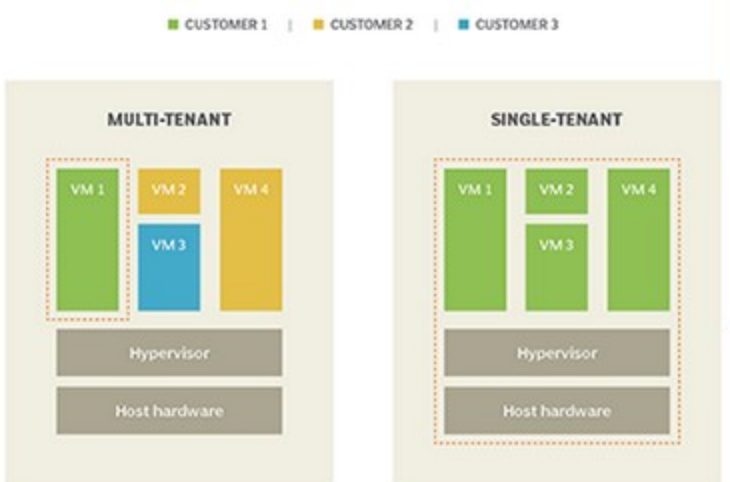
Quick Recap: Cloud Concepts, Architecture and Design

- Objective of the cloud is shift from CapEx to OpEx model
- Business needs of the organization drive security decisions and not the other way around.
- Funding and technology decisions for movement to the cloud should be made with the business direction

- The three main goals of information security are:
  - **Confidentiality** prevents unauthorized disclosure
  - **Integrity** prevents unauthorized alteration
  - **Availability** ensures authorized access

Quick Recap: Cloud Concepts, Architecture and Design

- **Cloud computing –** where computing services are being delivered to a customer at a remote location over a network.
- CPU, RAM, storage, and networking are **building blocks of cloud computing**
- The key characteristics of the cloud include:
  - On-demand self-service computing
  - Broad network access
  - Multitenancy
  - Rapid elasticity and scalability
  - Resource pooling
  - Measured service



Quick Recap: Cloud Concepts, Architecture and Design

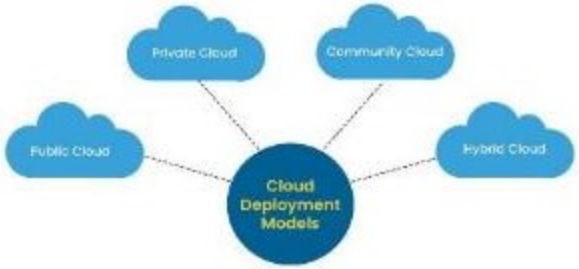
- **Cloud resources** may be rapidly provisioned and released with minimal service provider interaction.

Cloud Service Model:

Service Category	Description
Infrastructure as a Service (IaaS)	Cloud provider offers customers basic building blocks of compute, storage, and networking.
Platform as a Service (PaaS)	Cloud provider offers customers a platform upon which they can execute their own code.
Software as a Service (SaaS)	Cloud provider offers customers a complete application, ready to use and delivered over the Internet.

Cloud Deployment Model:

Deployment Model	Description
Public	Services offered to any customer in a shared environment
Private	Services operated for a single customer in a dedicated environment
Hybrid	Strategy mixing the use of public and private cloud resources
Community	Services offered to members of a closed group of customers



Quick Recap: Cloud Concepts, Architecture and Design

- DoS/DDoS threats and risks are not unique to the public cloud model
- DDoS attacks do not affect the productivity but rather availability for cloud customers.
- **Private Cloud** may be internal or external to an organization
- The primary benefit to the customer of using Infrastructure as a Service (IaaS) is the transfer of cost of ownership
- Security controls and countermeasures may reduce the financial benefits when to move cloud

Quick Recap: Cloud Concepts, Architecture and Design

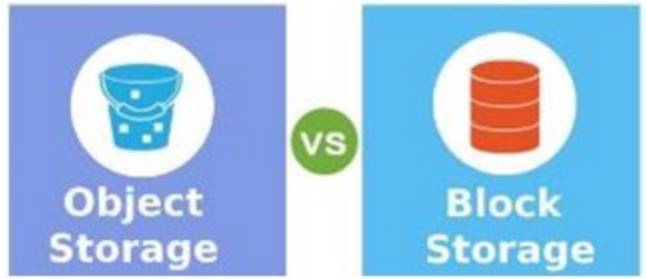
- **Ownership retention** is a unique benefit of the private cloud model
- Physical hardware costs would be most beneficial to a new company starting
- Roles in cloud computing include:
  - **Cloud Service Providers (CSP) –** offer computing services to third parties
  - **Customers** – consume services from providers
  - **Cloud Service Partners –** Offer third-party services that interact with CSP offerings
  - **Cloud Broker –** Provides service intermediation, aggregation, and arbitrage
  - **Cloud access security brokers (CASB) –** Offer cross- cloud managed identity and security services for cloud customers
  - **Cloud carrier –** Intermediary providing connectivity and transport of cloud services between provider and consumer

Quick Recap: Cloud Concepts, Architecture and Design

- The primary mechanisms for delivering cloud compute resources include virtual machines, serverless computing, and containers
- Public cloud environments are built upon the principle of **multitenancy**

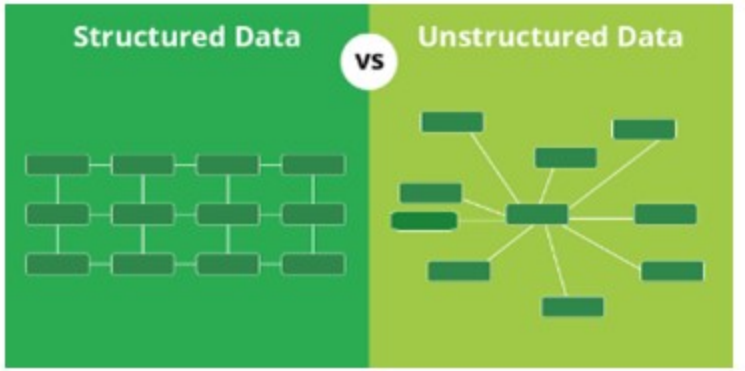
- Elimination of risks is not possible even with cloud migration
- **Transparency** is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences.
- **Reversibility** is the cloud concept involving the ability for a cloud customer to remove all of its data and IT assets from a cloud provider

Quick Recap: Cloud Concepts, Architecture and Design

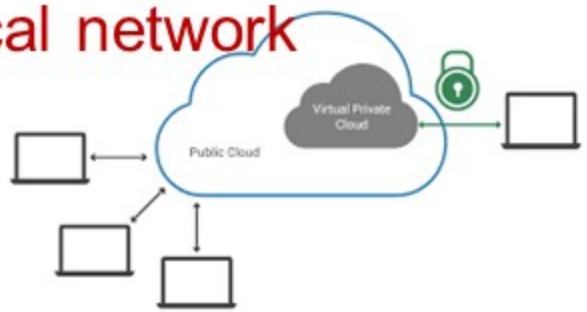


- **Block storage** provides virtual disk volumes for use by virtual machines. It uses iSCSI protocol
- **Object storage**
  - Is less expensive, flat and allows to store files as individual objects but can't be directly mounted by an operating system.
  - Access via APIs or web interface
  - Is a type of IaaS storage where files and objects are physically stored on a separate system and are referenced by a key or token value
  - Is the most likely type of storage used for virtual images
  - The user/administrator is limited to uploading, storing, and manipulating files (objects) as opposed to installing and running programs
  - Object storage uses a flat file system to hold storage objects
- The volume and object storage types are used within the Infrastructure as a Service model

Quick Recap: Cloud Concepts, Architecture and Design

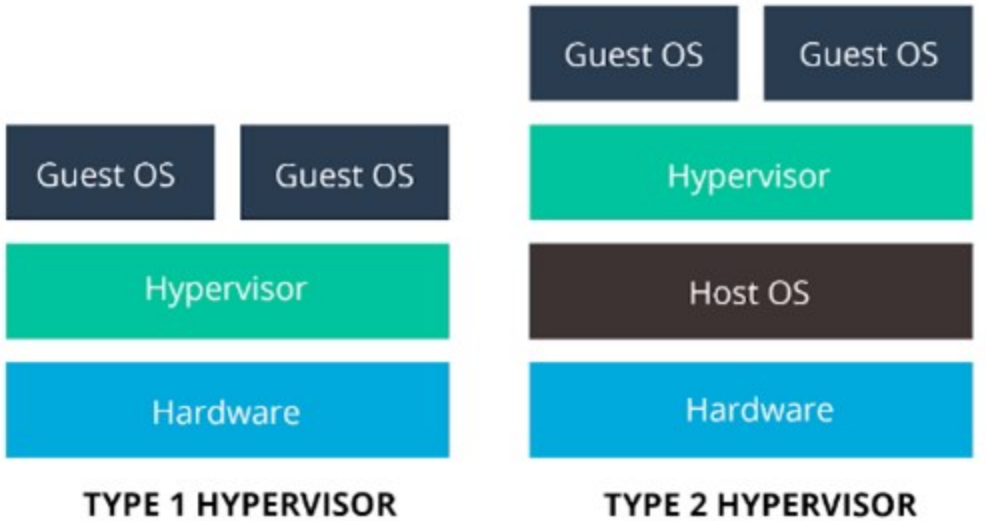


- **Structured data –** Information with a high degree of organization, such that inclusion in a relational database
- **Unstructured data –** Information that does not reside in a traditional row-column database. Unstructured data files often include text and multimedia content
- **Structured** and **unstructured storage** types are used in the Platform as a Service model
- **Data Fluidity –** Data is fluid in Cloud computing (on-Prem to off-Prem)
- **Virtual private clouds (VPCs)** are similar to VLANs on a physical network
- **PaaS** uses databases and Big Data storage types
- iSCSI does not natively support encryption



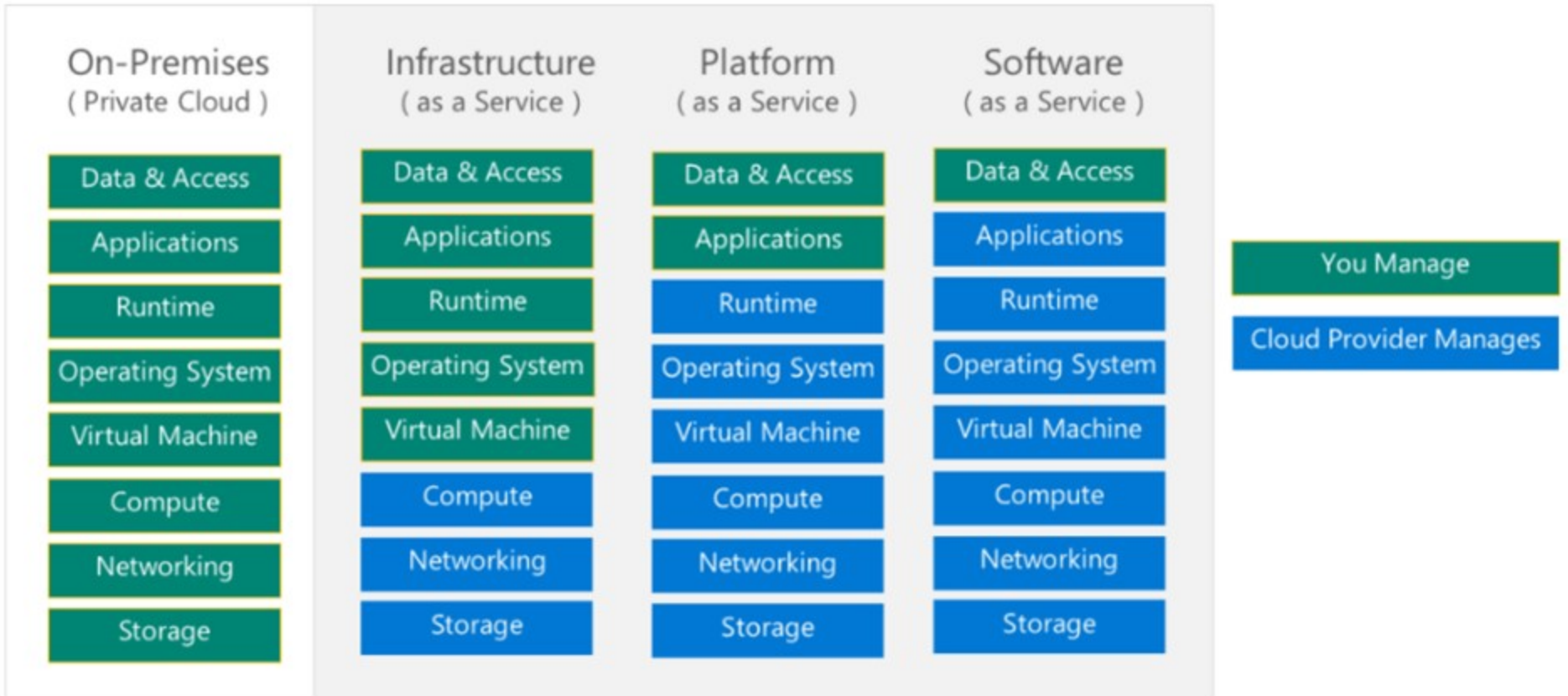
Quick Recap: Cloud Concepts, Architecture and Design

- **Type 1 vs. Type 2 Hypervisor**
  - Running on top of another operating system versus being tied directly to the hardware is a major security risk with Type 2 hypervisors
- In a virtualized environment, the hypervisor is responsible for enforcing isolation
- **Reservations** are a guaranteed minimum level of resources available to allocate to a host to power on and perform tasks
- The maximum level of resources available for allocation would refer to limits



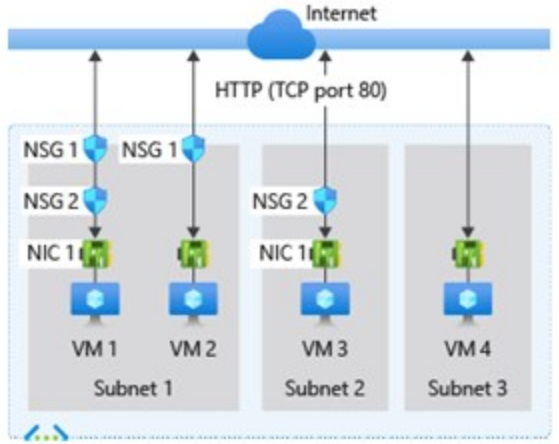
Quick Recap: Cloud Concepts, Architecture and Design

- Security in the cloud follows the **shared responsibility model** where vendors and customers have different responsibilities depending upon the category of cloud service



Quick Recap: Cloud Concepts, Architecture and Design

- Access to cloud resources can be controlled via use of **network security groups** which implement firewall-like functionality
- **Orchestration –** The goal of cloud orchestration is to automate the configuration, coordination, and management of software and its interaction
- **Cloud orchestration** allows the automation of administrative tasks including the creation of workloads, assignment of permissions, and provisioning of accounts. This builds upon the concept of **Infrastructure as Code**



Quick Recap: Cloud Concepts, Architecture and Design

- **Cloud provisioning –** Deployment of a company's cloud computing strategy. Determines services in the public cloud and which will remain on site
- **Management Plane** – Allows admin to manage any or all of the hosts remotely

- **Management Plane Breach** – Most significant risk in a managed cloud environment
- **Forklifting** – Process of migrating entire app the way it runs in a traditional environment with minimal code changes. Not all the application are Cloud Ready

- **Virtual machine introspection (VMI)** – Allows for agents less retrieval of the guest OS state (running Process, active network connection)

Quick Recap: Cloud Concepts, Architecture and Design

- **Interoperability** is the desire for compatibility of services between cloud service providers. Interoperability is the ability to split up and reuse components throughout systems and applications
- **Portability** is the ability to move workloads between providers with minimal effort. Portability refers to the ability to move systems and applications easily between different cloud providers
- **Containerization** supports portability by packaging workloads in a standardized manner
- **Resiliency** is the ability of a cloud service to withstand potentially disruptive events

Quick Recap: Cloud Concepts, Architecture and Design

- **ISO 27017** offers an international standard for cloud computing security that organizations may voluntarily adopt
- **NIST SP 800-145** defines the cloud concepts and definitions
- **PCI DSS** is a set of mandatory security requirements for organizations involved in credit card processing
- **Common Criteria or CC is international set of guidelines** and specifications s for evaluating IS products to ensure they meet security standards for government entities. It need to be verified by vendor neutral 3rd party. It tells how much thoroughly the product has been tested
- Federal government agencies require that services they use be certified under the Common Criteria (CC) and that encryption used to support them be compliant with FIPS 140-2

Common Criteria

FIPS 140-2

Quick Recap: Cloud Concepts, Architecture and Design

- **FedRAMP** is a regulatory framework that the United States federal government uses to assess and certify cloud services for their use by federal agencies

- **ISO/IEC 27001:2013** is commonly applied to cloud computing security as a standard and certification system for promoting and continually improving upon the security applied to a system or application. It does not recommend any technology

ISO/IEC 27001:2013

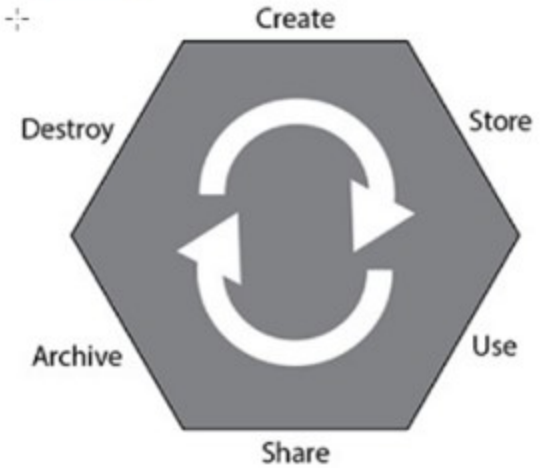
- **Availability** is the percentage of the time that a service is operating normally. Increased resiliency drives increased availability.

- Organizations may formalize availability requirements in written **Service Level Agreements (SLAs)**

Quick Recap: Cloud Concepts, Architecture and Design

- **Data lock-in** would make it very difficult for a customer to easily move to another cloud provider

- **Data Life Cycle**:
  - Create > Store > Use > Share > Archive >Destroy
  - This is not truly a cycle because data does not continue after the destroy phase



- **Lock-in/Vendor Lock-in –** Customers are bound to stay with a service provider due to situations like using proprietary format or unfavorable contractual agreements
- **Vendor Lock-out –** Customer is unable to recover or access their own data due to the cloud provider going into bankruptcy or otherwise leaving the market

Quick Recap: Cloud Concepts, Architecture and Design

- In all Cloud deployment/service models, one can assign/transfer responsibility but not necessarily accountability
- **Shares** is a prioritization and weighting system within a cloud environment that sets that order of specific applications or customers to receive additional resources when requested
- **Cloud Bursting –** Is all about dynamic deployment of applications that normally run on a private cloud into a public cloud to meet expanding capacity requirements and handle peak demands when private cloud resources are insufficient

Quick Recap: Cloud Concepts, Architecture and Design

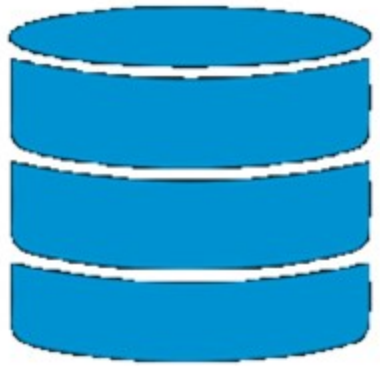
- **Shadow IT** – occurs when cloud users access and use cloud systems and resources that have not been authorized by their organization.

Cloud Data Security

Domain 2

Quick Recap: Cloud Data Security

- **Raw disk storage** is permanently allocated storage that exists independently of a server instance.
- **Ephemeral storage** is temporary storage associated with a specific instance that is destroyed when the server is stopped.
- 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.
- Some CSP provides tailored services to store archived data that enterprises can access by using API (Write Once Read Many)

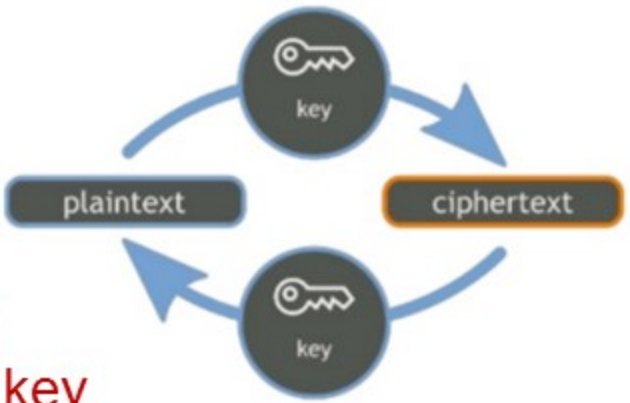


Quick Recap: Cloud Data Security

- **Data dispersion –** data should be stored in geographically disparate locations to protect against regional disruptions
- Cloud service providers provide replication services that allow automated data dispersion
- **Data dispersion** can't aid in inadvertent loss caused by an errant user; if the user accidentally deletes/corrupts a file
- **Bit Splitting –** Splitting up and storing encrypted information all across cloud storage.
- **Erasure coding –** is the technology in which segments of data are encrypted and dispersed across the network and makes dispersion possible
- **Erasure coding** is the practice of having sufficient data to replace a lost chunk in data dispersion

Quick Recap: Cloud Data Security

- **Cryptography** uses mathematical techniques to prevent unauthorized individuals from viewing data. It consists of two operations:
  - **Encryption** transforms plaintext into ciphertext using an encryption key
  - **Decryption** transforms ciphertext back into plaintext using a decryption key

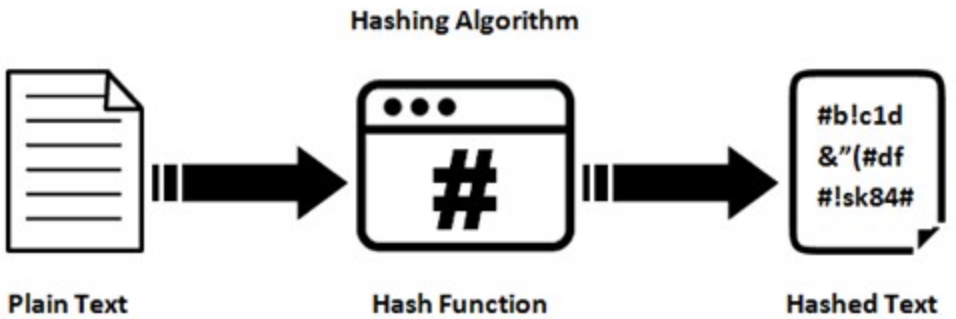


- The **goals** of cryptography are:
  - **Confidentiality** to protect information from unauthorized access
  - **Integrity** to protect information from unauthorized changes
  - **Authentication** to provide proof of identity claims
  - **Non-repudiation** to provide the ability to prove the origin of a message to a third party.

Quick Recap: Cloud Data Security

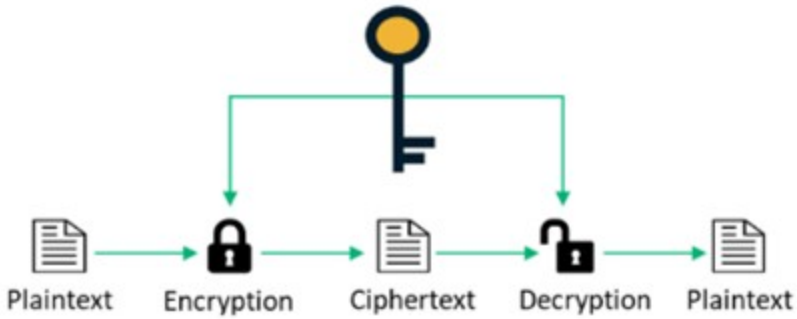
- **Cryptographic keys** should not be stored along with the data they secure, regardless of key length
- **Customer** should own & posses keys and key management
- **Single person** should never handle encryption
- **Separation of Duties** (**SoD**) should be followed
- **Key management** should be separated from CSP

- **Hashes** are one-way functions that produce a unique value for every input and cannot be reversed
- **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 customer.



Quick Recap: Cloud Data Security

- **Symmetric encryption** uses the same shared secret key for encryption and decryption
  - Secure symmetric algorithms include 3DES, AES, IDEA, and Blowfish. DES is not secure
- In **asymmetric encryption**, users each have their own public/private keypair
  - Secure asymmetric algorithms include RSA, El Gamal, and elliptic curve (ECC)
- Encryption keys should not be accessible to the cloud service provider
- The **Diffie-Hellman** algorithm may be used for secure exchange of symmetric keys



Quick Recap: Cloud Data Security

- **Transparent encryption –** is part of the database and not known to the user; it is integrated with the actual database processes and works as part of the ongoing workflow. Specific tables within the database can be encrypted using this.
- **File-level encryption –** Encrypting volume or folder of Database with the encryption engine and keys residing on the instance

- **Application-level encryption –** Encryption engine resides at application that is utilizing the database
- Core components to an encryption system architecture:
  - Software
  - Data
  - Keys

Quick Recap: Cloud Data Security

- **IaaS Encryption –** uses Volume Storage Encryption and Object Storage Encryption
- **PaaS Encryption** – Client/Application Encryption, Databased encryption and proxy-based encryption
- **SaaS Encryption –** is managed by the Cloud Service Provider by the applications and through Proxy encryption

Quick Recap: Cloud Data Security

- **Digital rights management (DRM)** was designed to focus on security and encryption as a means of preventing unauthorized copying and limitations on distribution of content to only those authorized (purchasers).
- **Enterprise digital rights management**, also known as information rights management (IRM), is a subset of DRM and typically refers to business-to-business securing of information rights.

- **DRM** is focused specifically on the protection of consumer media, such as publications, music, movies, and so on. **IRM** is used to protect general institution data, so financial records, personnel data, and security profiles would all fall under the auspices of IRM.
- **DRM** should enforce dynamic policy control, audit logs, automatic expiration, support existing authentication infrastructure

Quick Recap: Cloud Data Security

- **Digital certificates** use the X.509 standard and contain a copy of an entity's public key. They are digitally signed by a certificate authority (CA).
- **Hardware security modules (HSMs)** are dedicated hardware devices used to manage encryption keys and perform cryptographic operations
- **FIPS 140-2** is a certification for cryptographic modules based on the specific needs and requirements for the level of encryption and the protection of it. It certifies cryptographic modules for unclassified data processing

FIPS 140-2 Level	Controls
Security Level 1	Standard operating systems, no physical security
Security Level 2	EAL2 software and firmware, tamper- evident seals
Security Level 3	EAL3 software and firmware, tamper- resistant controls
Security Level 4	EAL2 software and firmware, strict physical security

Quick Recap: Cloud Data Security

- To create a digital signature the sender of a message performs the following steps:
  1. Generate a message digest using a hash function
  2. Encrypt the message digest with the sender's private key to create a digital signature
  3. Attach the digital signature to the message
- To verify a digital signature, the recipient of a message performs the following steps:
  1. Decrypt the digital signature using the sender's public key
  2. Generate a message digest of the message using the same hash function used by the sender
  3. Compare the decrypted digital signature from step 1 with the hash generated in step 2. If they match, the message is authentic

Quick Recap: Cloud Data Security

- **Cloud-based systems** and applications are heavily dependent on encryption for virtually all communications and storage systems

- **Availability** of the key management system is vital for any applications and access to work in order to make data available

Quick Recap: Cloud Data Security

- **Certificates** may be revoked using two techniques.
  - Inclusion of the certificate serial number on a **certificate revocation list (CRL)**
  - Provide certificate users with access to certificate status in real-time using the **Online Certificate Status Protocol (OCSP)**
- **Transport Layer Security (TLS)** is the replacement for Secure Sockets Layer (SSL) and uses public key cryptography to exchange a shared secret key used to secure web traffic and other network communications.

- TLS used two layers:
  - **TLS Handshake Protocol -** negotiates and establishes the TLS connection between the two parties
  - **TLS Record Protocol** - actual secure communications method for transmitting of data.
- TLS uses a new symmetric key for each secure connection

Quick Recap: Cloud Data Security

- **Deidentification** removes obvious identifiers from a data
- We can perform secure deidentification by having a statistician validate your deidentification work
- **Anonymization** involves replacing data so that it cannot be successfully mapped back to an individual

Obfuscation Technique	Description
Hashing	Replaces sensitive data elements with hashed values generated using a one-way function
Masking	Replaces some or all characters of a sensitive data element with blank values, such as "*" or "X"
Tokenization	Replaces sensitive fields with a random identifier that may be reversed using a secured lookup table
Scrambling	Mimics the look of real data, but simply jumbles the characters into a random order.

Quick Recap: Cloud Data Security

- **Static data masking –** A process of duplicating the original data with sensitive components masked in the new copy. Static masking is the better option when you need to use "real" data in a development or test environment.

- **Dynamic data masking –** Dynamic masking is the process of masking sensitive data as it is used in real-time, rather than creating a separate masked copy of the data. This method is sometimes referred to as on-the-fly masking, and requires a masking layer in between the storage component and the application.

Test data generation: This is the creation of a database with non-sensitive test data based on a "real" database. It can use scrambling and other randomization techniques to create a data set that resembles the source in size and structure but lacks sensitive data.

Quick Recap: Cloud Data Security

- **Data loss prevention (DLP)** help to prevent sensitive information from exfiltration, blocking it to keep information secure
- Information should be classified based upon its sensitivity to the organization
  - On the user's device is the correct choice of data-in-use monitoring
  - Integrated with the database server would provide coverage for data at rest
  - Network boundary would provide coverage for data in transit

- Biggest challenge for protecting data at rest with DLP is resource pooling
- DLP Solution can locate data assets according to criteria defined by the organization

- DLP solutions works with Digital rights management (DRM) to protect the data

Quick Recap: Cloud Data Security

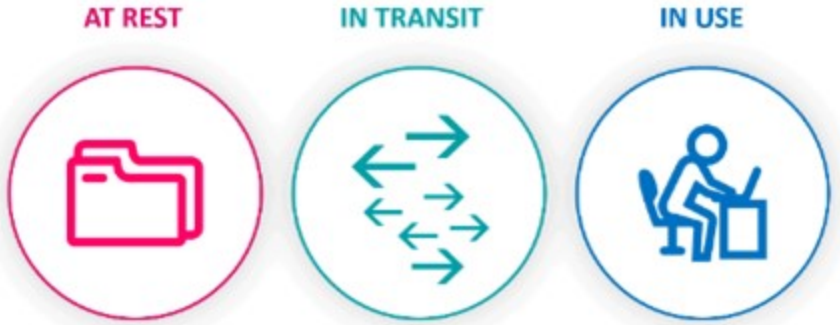
- **Erasing** performs a delete operation on a file but the data remains on disk
- **Clearing overwrites** the data with random values to ensure that it is sanitized.
- Common classes of sensitive information include:
  - **Personally identifiable information (PII) –** uniquely identifies individuals
  - **Protected health information (PHI) –** uniquely identifies individual health records
  - **Proprietary information –** contains trade secrets
- Legally and financially, in the eyes of the court, organization is always responsible for any unplanned release of PII
- **Cryptographic erasure –** in which the encryption keys are deleted as a means to protect and destroy data, available in cloud environment as well

Quick Recap: Cloud Data Security

- **Crypto-shredding** is the practice of deleting data by deliberately deleting or overwriting the encryption key
- Crypto-shredding requires two cryptosystems: one to encrypt the target data, the other to encrypt the resulting data encryption keys
- Crypto-shredding relies on the destruction of the final keys

Quick Recap: Cloud Data Security

- Different **data state**:
  - **Data at Rest:** Data stored on a system or media device
  - **Data in Motion**: Data in transit over a network
  - **Data in Use:** Data being actively processed in memory



- **Data in Use** is the most vulnerable for misuse/leak
- Information should be labeled with its classification
- Data classification is the responsibility of the data owner
- **Security controls** should be defined and appropriate for each classification level

- **Data labels** does not include the *value of data*, it can include *date on which data was created, data owner, date of scheduled destruction, handling restrictions, jurisdiction, confidentiality level, distribution limitations etc.*

Quick Recap: Cloud Data Security

- Data transforming from raw objects to virtualized instances snapshotted images and vice-versa may affect the organization's current classification methodology
- Collect only data that is necessary for legitimate business purposes. This is known as **data minimization**

- Data should be retained no longer than necessary. Use sanitization technology to ensure that no traces of data remain on media (**data remanence**) before discarding it.
- **Data remanence** are residual representations of data that remain after deleting files or reformatting data storage devices

- **Homomorphic** is experimental technology that allows a system or application to read and manipulate encrypted data without first having to unencrypt it

Quick Recap: Cloud Data Security

- **Data Roles**:
  - **Data Owner** – Senior-level executive who establishes rules and determines controls
  - **Data Subject –** Individual with personal data
  - **Data steward –** Responsible for overseeing an organization's policy in regard to data access, evaluating access requests and to ensure compliance and proper use
  - **Data Controller –** Determines the purpose and manner that the personal data will process
  - **System Owner –** Individual responsible for overseeing secure operation of systems
  - **Data Processor –** Individual with access to personal or sensitive information

Quick Recap: Cloud Data Security

- The major categories of **intellectual property protection** include:
  - **Trademarks –** protect words and symbols.
  - **Copyrights –** protect creative works
  - **Patents –** protect inventions
  - **Trade secrets –** require maintaining secrecy but don't expire

- Strong contract language ensure protection of intellectual property created in the cloud

Quick Recap: Cloud Data Security

- **Legal holds –** require the preservation of relevant electronic and paper records
- Organizations may be required to collect and produce information to the other party in the dispute through an **electronic discovery** (or **eDiscovery**) process
- **ISO/IEC 27050 –** is a standard focused on eDiscovery processes and how best to approach an order
- **ISO/IEC 17789 –** provides a reference architecture for cloud computing and is focused on general cloud computing design and implementation
- **Chain of Custody –** If evidence may be used in court, forensic analysts should document every step of the collection, analysis, and storage process
- A break in the chain of custody makes the evidence inadmissible in the court

Quick Recap: Cloud Data Security

- **Security information and event management (SIEM)** systems aggregate logs from diverse systems, serving as a central, secure collection point.
- **Availability of Logs in SaaS (no control of customers)**
  - Web server logs, Application server logs, Database logs, Guest OS logs, Host access logs, Virtual logs, Network captures, Billing records
- **Availability of Logs in PaaS (some control to customer)**
  - Input validation failures, Authentication success and failures, Authorization failures, Session management failures, High-risk functionality (e.g., privileged user access, network connection, key exchanges), Legal and other opt-ins

- **Availability of Logs in IaaS (customer has control of data):**
  - Cloud network logs, DNS server logs, VM logs, Host OS and Hypervisor logs, API access logs, Management portal logs, Packet captures, Billing records
- **Log injection attack** occurs when an attacker creates false log entries or injects malicious content into logs through un-validated input

Cloud Platform and Infrastructure Security

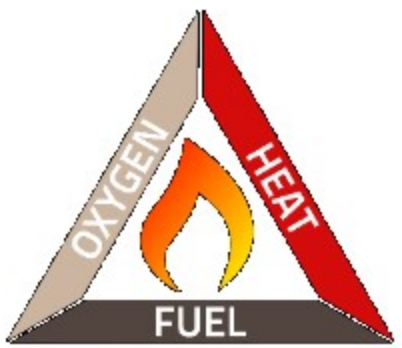
Domain 3

Quick Recap: Cloud Platform and Infrastructure Security

- Secure the management plane, restrict the administrative access to underlying systems and hardware
- Power issues in physical environment:

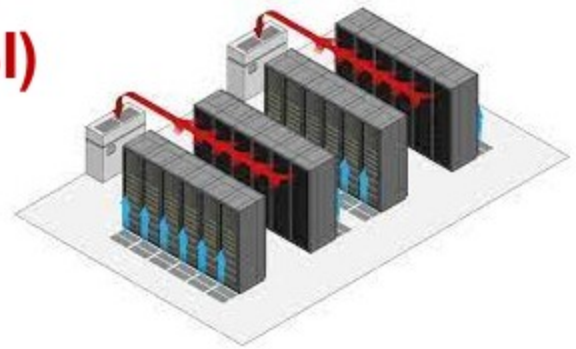
Power Issue	Brief Duration	Prolonged Duration
Loss of power	Fault	Blackout
Low voltage	Sag	Brownout
High voltage	Spike	Surge
Disturbance	Transient	Noise

- Fires require the combination of heat, oxygen, and fuel. They may be fought with fire extinguishers. Different classes of fire are:
  - **Class A:** common combustible fires
  - **Class B:** liquid fires
  - **Class C:** electrical fires
  - **Class D:** metal fires

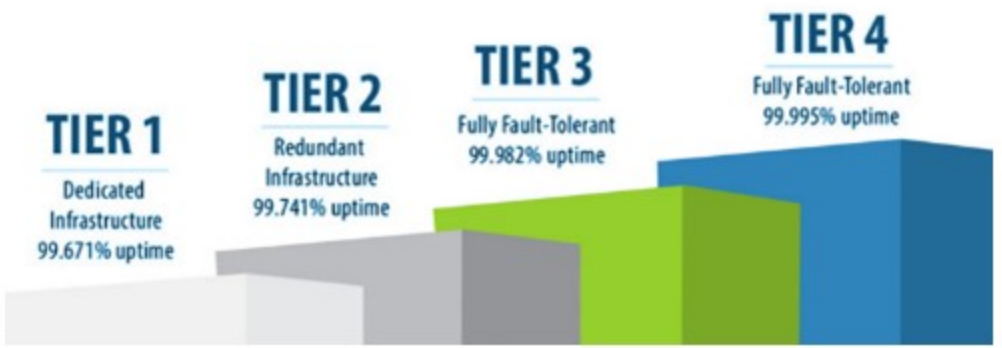


Quick Recap: Cloud Platform and Infrastructure Security

Data Centers Design Standards



- **Building Industry Consulting Service International INC (BICSI)**
  - Cabling and Design installation
- **The International Data Center Authority (IDCA)**
  - Data center location, facility structure, and infra-structure and application
  - Takes a macro-level approach to data center design
- **National Fire Protection Association (NFPA)**
  - Requirement for temperature, emergency
- **Uptime Institute**
  - Standard on data center tiers and topologies
- **Tier 3** – requirement of **Concurrently managed**
- **Tier 4** – requirement of **Fault tolerant**



Quick Recap: Cloud Platform and Infrastructure Security

- Data Center needs to be between **64 and 81 degrees** F. Thermostat on return air may result in high energy costs
- Data Center needs to be between **40 and 60 percent** of humidity. Too low increases static, too high increases corrosion and bio creep
- **Chicken Coop Data center** – Long side facing the prevailing wind to allow for natural cooling
- A generator transfer switch should bring backup power online before the UPS duration is exceeded
- UPS should last long enough for graceful shutdown of affected systems

Quick Recap: Cloud Platform and Infrastructure Security

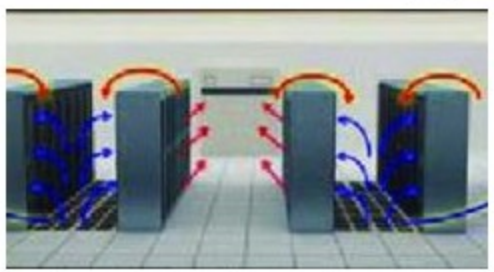
- **Data Center Redundancies**:

External Redundancy	Internal Redundancy
Power Feeds/Lines	Power Distribution Unit
Power Substations	Power Feeds to Racks
Generators	Cooling Chillers and Units
Generator Fuel Tanks	Networking
Network Circuit	Storage Unit
Building Access Points	Physical Access Points
Cooling Chilling Infrastructure	

Quick Recap: Cloud Platform and Infrastructure Security

- **Wet pipe fire suppression systems** – always contain water
- **Dry pipe systems** – only fill with water when activated
- **Preaction systems** – fill the pipes at the first sign of fire detection
- **Mantraps** use a set of double doors to restrict physical access to a facility

- **Hot and cold aisle** approaches manage cooling by aligning data centers so that the front of one row of server faces the front of the adjacent row (cold aisle) and the backs
- Power distribution units are internal to a data center

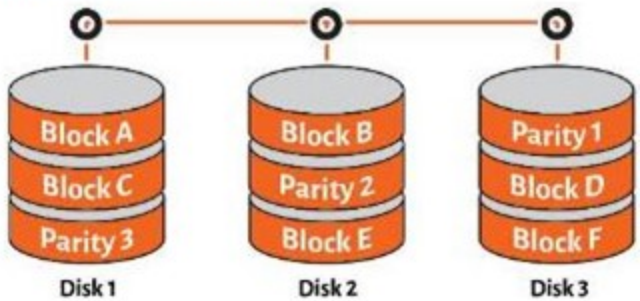


Quick Recap: Cloud Platform and Infrastructure Security

- **Business continuity plans (BCP)** seek to make a business resilient against disruptions, allowing it to continue operations despite adverse circumstances
- A **qualitative assessment** is based on a review of documentation in regard to system design, policies, and procedures
- **Quantitative assessment** is based on hard numbers or data

Quick Recap: Cloud Platform and Infrastructure Security

- **BCP steps –** Define, Analyze, Assess Risk, Design, Implement, Test
- Continuity can be achieved by preventing disruptions
  - **High availability (HA)** uses multiple systems to protect against service failure, such as clustering servers.
  - **Fault tolerance (FT)** makes a single system resilient against technical failures, such as installing redundant disks or power supplies
- **RAID**, redundant arrays of inexpensive disks, is a fault tolerance mechanism for storage, protecting against the failure of a single disk.



  - **RAID 1,** also known as **disk mirroring**, stores the same data on two different disks.
  - **RAID 5,** also known as **disk striping with parity**, uses three or more disks to store data and parity information.

Quick Recap: Cloud Platform and Infrastructure Security

- **Backups** are recovery control, allowing the restoration of data
- There are **three major** categories of backup.
  - **Full Backup**: Copies all files on a system.
  - **Differential Backup:** Copies all files on a system that have changed since the most recent full backup.
  - **Incremental Backup:** Copies all files on a system that have changed since the most recent full or incremental backup.

- Location of stored data would be the most important concern from a regulatory standpoint due to different jurisdictions and requirements
- Disaster recovery sites fit into **three major categories**

Site Type	Support Systems	Configured Servers	Real-time Data
Cold Site	Yes	No	No
Warm Site	Yes	Yes	No
Hot Site	Yes	Yes	Yes

Quick Recap: Cloud Platform and Infrastructure Security

- Disaster recovery plans require testing. There are **five major test types**:

Read-through/ tabletop	• Participants review the plan and their specific role, either as a group or individually.
Walkthrough	• The DR team gathers to walk through the steps in the DR plan and verify that it is current and matches expectations.
Simulation	• DR team participates in a scenario-based exercise that uses the DR plan without implementing technical recovery controls.
Parallel	• DR team activates alternate processing capabilities without taking down the primary site.
Full interruption	• DR team takes down the primary site to simulate a disaster.

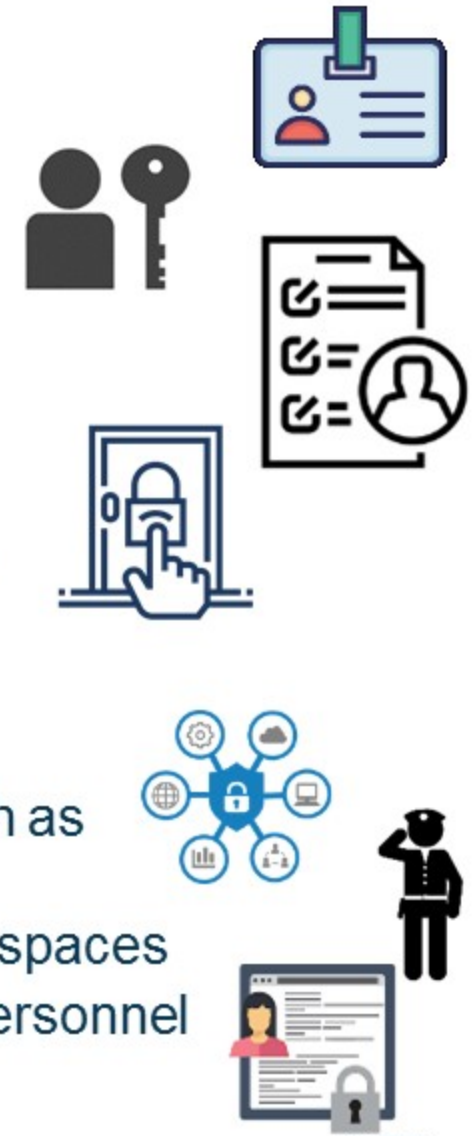
Quick Recap: Cloud Platform and Infrastructure Security

- Upon major configuration changes, BCDR should be tested
- The **recovery point objective (RPO)** sets and defines the amount of data an organization must have available or accessible to reach the determined level of operations necessary during a BCDR situation.

- The **recovery time objective (RTO)** measures the amount of time necessary to recover operations to meet the BCDR plan.
- **Software-Defined Networking (SDN) –** Decouple **Control Plane (Filtering)** and **Data (forwarding) Plane**
- **BCDR Plan –** Define scope, gather requirements, assess risk, implement

Quick Recap: Cloud Platform and Infrastructure Security

- The core activities of identity and access management are:
  - **Identification** where a user makes a claim of identity.
  - **Authentication** where the user proves the claim of identity.
  - **Authorization** where the system confirms that the user is permitted to perform the requested action.
- For access controls, limit the access that subjects (e.g. users, applications, processes) has on objects (e.g. information resources, systems)
- Access controls are of **three types**:
  - **Technical (or logical) controls** use hardware and software mechanisms, such as firewalls and intrusion prevention systems, to limit access
  - **Physical controls**, such as locks and keys, limit physical access to controlled spaces
  - **Administrative controls**, such as account reviews, provide management of personnel and business practices



Quick Recap: Cloud Platform and Infrastructure Security

- **Zero Trust Architecture (ZTA) -** is a security model that's built on the idea that no entity inside or outside of an organization's security perimeter should be trusted

Cloud Application Security

Domain 4

Quick Recap: Cloud Application Security

- The **Security Assertion Markup Language (SAML)** allows browser-based single sign on across a variety of systems. Its XML based framework. There are **three entities** in a SAML relationship:
  - The **principal** is the end user.
  - The **identity provider** is the organization providing the user's account that is used for authentication.
  - The **service provider** is the organization offering the service requested by the end user
- The **Secure Software Development Lifecycle (SDLC)** creates a formal process for software development in an organization.
- **Software Development Life cycle** – Planning, requirements gathering, defining, designing, developing, testing, and maintenance
- The spiral model uses a more iterative approach

Quick Recap: Cloud Application Security

- In define phase, users inputs are requested.
- In design phase, the business requirements are mapped to system designs
- Security personnel should be involved in define phase.

Quick Recap: Cloud Application Security

- The **Agile methodology** is a way to manage a project by breaking it up into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage. Following are features:
  - Individuals and interactions instead of processes and tools
  - Working software instead of comprehensive documentation
  - Customer collaboration instead of contract negotiation
  - Responding to change instead of following a plan

- The **DevOps model** of IT seeks to better integrate the development of code and the operation of IT infrastructure.

- Security should be involved at very initial stages of requirement gathering
- **Verification** and **validation** should occur at each stage of the SDLC

Quick Recap: Cloud Application Security

- The goal of **threat modeling** is to determine any weaknesses in the application and the potential ingress, egress, and actors involved before the weakness is introduced to production
- **DREAD** Model
  - Focuses on a quantitative value for assessing risks and threats.
  - With a quantitative value, it can be compared with other systems and even itself over time.
  - Risk_DREAD = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5

- **STRIDE Model**
  - Threat classification scheme
  - *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege*

Quick Recap: Cloud Application Security

- **Change and configuration management** processes ensure that organizations have standardized processes in place for requesting changes, implementing those changes, and releasing code to productions.
  - **Request control** manages, evaluates, and prioritizes inbound requests from customers
  - **Change control** grants permission for developers to make changes to application code
  - **Release control** moves code from the development environment into production
- **Puppet** is a tool for maintaining configurations and deployments across systems and applications, as well as for enforcing rules and requirements for the configurations.

puppet

- **Chef** is a software tool for handling infrastructure configurations. Automates the build, deploy, and manage infrastructure. Stores recipe as well as other configuration data

CHEF

Quick Recap: Cloud Application Security

- **Infrastructure as Code (IaC) –** allows developers to view and manipulate their IT environments directly from lines of code using a programming or configuration language

Quick Recap: Cloud Application Security

- Attack Types

Attack	Description
Cross-site scripting (XSS)	Places malicious scripts on a site that users visiting the site later execute. Takes advantage of reflected input.
Cross-site request forgery (CSRF/XSRF)	Attempts to execute commands against other logged-in sessions in a user's browser.
SQL injection	Sends SQL commands to a web application in an attempt to have them executed on the backend database server.
Privilege escalation	Seeks to elevate a normal user-level account into one with administrative privileges.
Directory traversal	Navigates a web server's file system by embedding ..'s and /'s in URLs.
Buffer overflow	Attempts to place more data in a memory location than fits there in an attempt to force the execution of malicious code.
Session hijacking	Steals a user's web cookie to take over an authenticated session.

Quick Recap: Cloud Application Security

- **Input validation protects** against many application attacks by sanitizing user input
- **Whitelisting** specifies the exact types of input that are allowed
- **Blacklisting** specifies malicious input types that are prohibited
- **Parameterized queries** use templates for database queries to prevent the inclusion of user-provided code
- **Stored procedures** are an implementation of parameterized queries
- **Code repositories** provide collaborative development tools and version control. They must be protected against unauthorized access

Quick Recap: Cloud Application Security

- **Code signing** uses **digital signatures** to demonstrate the authenticity of code to users installing it on their systems
- **Sandboxes** – isolated environments where developers can test code. It can be within the same environment

- **Application Virtualization** - Concept of isolating an application from the underlying operating system for testing purposes. It allows user interaction with sensitive data without transferring it to their device

Quick Recap: Cloud Application Security

- The **OWASP top 10** covers the following categories:
  1. Injection
  2. Broken Authentication and Session Management
  3. Cross-Site Scripting (XSS)
  4. Insecure Direct Object References
  5. Security Misconfiguration
  6. Sensitive Data Exposure
  7. Missing Function Level Access Control
  8. Cross-Site Request Forgery (CSRF)
  9. Using Components with Known Vulnerabilities
  10. Unvalidated Redirects and Forwards

Quick Recap: Cloud Application Security

- **12 most "treacherous" threats** to cloud security by **CSA**, risk specific to cloud based application and systems

1. Data Breaches
2. Insufficient Identity, Credential, and Access Management
3. Insecure Interfaces and Application Programming Interfaces (APIs)
4. System Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

Quick Recap: Cloud Application Security

- There are three major approaches to threat identification:
  - **Asset focused** approaches use the asset inventory as the basis for the analysis
  - **Threat focused** approaches identify how specific threats may affect each information system
  - **Service focused** approaches identify the impact of various threats on a specific service
- **Software testing** techniques - verify security and effectiveness of software
- **Software Testing** Technique:

  - **Validation:** Ensures that software meets business requirements. It answers the question "Are we building the right software?"
  - **Verification**: Ensures that software functions correctly. It answers the question "Are we building the software right?"
  - **Stress testing:** Uses automated scripts to verify system capacity.
  - **User Acceptance Testing (UAT):** Ensures that software will work for users by allowing them to verify functionality.
  - **Regression testing:** Checks for unexpected side effects of software changes.

Quick Recap: Cloud Application Security

- **Flaws vs. Bugs**
  - **Flaw**: Inherent fault with the design of code
  - **Bug**: Implementation fault

Quick Recap: Cloud Application Security

- **Software libraries** – consist of shared third-party code that may be used by developers
- **Software development kits (SDKs)** – are packages of libraries and other tools to help developers work with other systems
- **Application programming interfaces (APIs)** – allow developers to interact with web services
- **APIs** are often secured using API keys which should be carefully protected to avoid unauthorized access to the API
- APIs can differ greatly between cloud providers and, depending on how the applications are built or implemented, may make it difficult to seamlessly move from one environment to another

Quick Recap: Cloud Application Security

- **Representational State Transfer (REST)** and **Simple Object Access Protocol (SOAP)** are the two main types of APIs used within cloud-based systems.
  - **REST –** Software architecture style of guidelines and best practices for scalable web services - Supports many formats and uses HTTP. It relies on URI (Uniform Resource Identifier) – Faster. REST API TLS use to protect data transmissions
  - **SOAP –** protocol specification for exchanging structured info in the implementation or web services - It only supports XML – Slower. It must rely on the encryption for security.

Quick Recap: Cloud Application Security

- Cloud security controls often map directly to as of on premises security controls

- **Firewalls** – restricts network access to authorized connections. In cloud its implemented using security groups
- In an IaaS environment, cloud providers do not allow customers to interact directly with network firewalls. Security groups allows customers to restrict access to their server instances

- **Transport Layer Security (TLS)** – Encrypts data in transit over a network
- **Full disk encryption –** Protects data at rest on disks with encryption.

- **Web Application Firewall (WAF) –** Provides application-layer security fo web applications, filtering out potentially malicious HTTP requests.

Quick Recap: Cloud Application Security

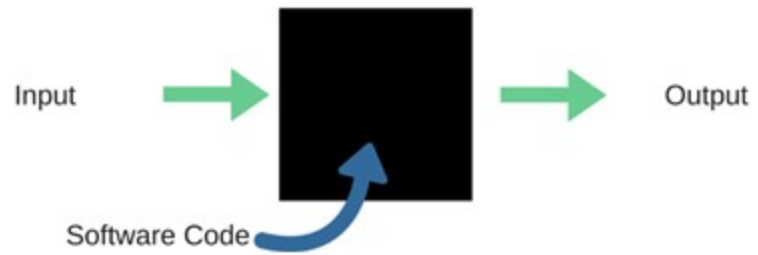
- **XML firewalls:** Most commonly deployed in line between the firewall and application server to validate XML code before it reaches the application. Filters requests to REST APIs for potential security issues

- **Database Activity Monitoring (DAM)** – Tracks, moderates, and analyzes access to sensitive databases by privileged and normal users. Can help to prevent SQL based attacks. It can be Host-based or Network-based

- **API Gateway** – Moderates access to APIs and enforces security requirements.
- TLS and IPSec can be used to prevent eavesdropping.

Quick Recap: Cloud Application Security

- **Static Application Security Testing (SAST)**
  - Also called White box testing. Performed without executing the application
  - Determines coding errors. Used in early development life cycle
  - Useful for XSS, SQL Injection, Backdoors
- **Dynamic Application Security Testing (DAST)**
  - Black box testing. Executed by running it
  - Useful to test exposed HTTP and HTML Interfaces



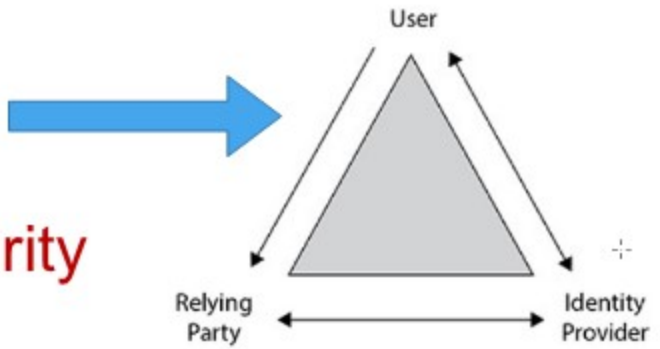
- **Runtime Application Self Protection (RASP)**
  - Considered to focus on application that possesses self-protection capabilities. Prevents attacks by self-protecting without human intervention
- **Runtime application self-protection (RASP)** would only be performed against systems that contain self-protection capabilities

Quick Recap: Cloud Application Security

- **Federation –** Process of linking an entity's identity across multiple separate identity management systems, like on-prem and cloud systems.
- **Federation** enables a cloud provider's identity system to trust an organization's existing identity profiles and attributes and use that identity information to manage access to cloud resources
- In Federation, members that participate run their own identity providers, and the systems that accept them are known as the relying party
- The identity provider and relying party are the two components
- Tokens are passed between systems, which enables the relying parties or service providers to verify back to the identity provider

Quick Recap: Cloud Application Security

- The typical relationship flow between the user, identity provider, and relying party is shown



- **WS-Federation** – Defines mechanism to allow different security realms to federate such as authorized access to resources
- **OpenID** – Lets developers authenticate their users across websites and apps

OpenID

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

Cloud Security Operations

Domain 5

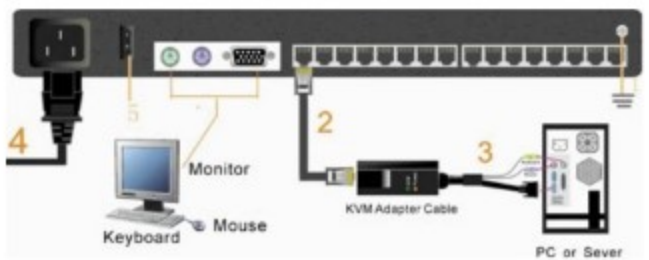
Quick Recap: Cloud Security Operations

- The **Basic Input Output System (BIOS)** is responsible for loading the operating system from disk when a computer boots. It is stored in firmware
- The **Unified Extensible Firmware Interface (UEFI) verifies** firmware before loading to confirm its integrity
- The **Trusted Platform Module (TPM)** is a hardware chip on the main board of the device that serves as the UEFI root of trust, protects encryption keys, and verifies hypervisor integrity in a virtualized environment

- TPM has full disk encryption capability. It has unique RSA key burned into it
- TPM also perform tasks as a **cryptoprocessor**

Quick Recap: Cloud Security Operations

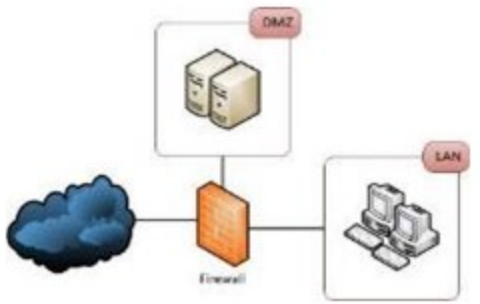
- A **hardware security module (HSM)** is a physical computing device that provides crypto processing and safeguards and manages digital keys for strong authentication
- **HSM (Hardware Security Module)** – Manages, generates, and stores crypto keys
- Review of HSMs are done by an independent lab



- KVM solutions provide keyboard, video, and mouse service to many servers located in a data center from a single physical or virtual location
- Administrators may access Windows systems using the Remote Desktop Protocol (RDP) which runs on TCP port 3389. Linux systems may be accessed using the Secure Shell (SSH) protocol on TCP port 22

Quick Recap: Cloud Security Operations

- **Defense-in-depth –** Organizations should use a variety of overlapping security controls to prevent against the failure of a single control. When designing overlapping controls, strive for diversity of vendors and control types

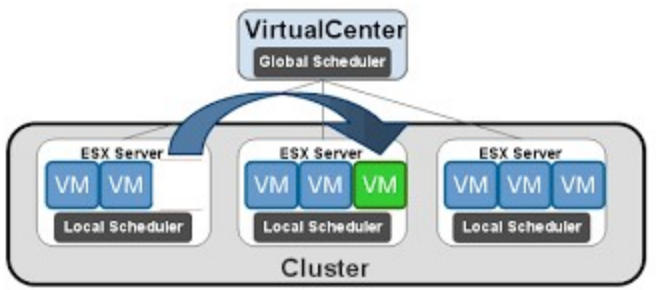


- Mostly firewall use **three zones**: a **trusted intranet**, an **untrusted Internet**, and a **demilitarized zone (DMZ)** that houses **publicly accessible servers**.
- When managing security of a system, keep in mind the following operating system security principles:
  - Disable unnecessary services and applications
  - Close unneeded network ports
  - Disable default accounts and passwords
  - Apply all security patches

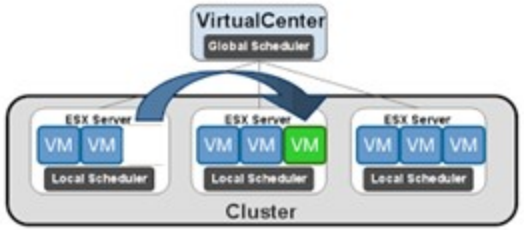
Quick Recap: Cloud Security Operations

- **Patching** in a cloud environment is typically performed by reimaging hosts from the new
- Simply powering off a VM still leaves the image files susceptible to malware infections and missed patching

- **Load balancers** – distribute connection requests among many identical servers.
- **Virtualized clusters** increase the flexibility of high availability approaches
- **VMware** uses distributed resource scheduling to allow the balancing of capacity across devices



Quick Recap: Cloud Security Operations



- **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.
- **Dynamic optimization strategies** allow the automated shifting of workloads. It ensure that resources are available when and where needed and that physical nodes do not become overloaded or near capacity while others are underutilized

- **Maintenance mode** allows taking hardware out of a virtualization pool temporarily while it is repaired.

Quick Recap: Cloud Security Operations

- **Firewalls** are the primary network security control used to separate networks of differing security levels
- TLS to be used to secure network communications. SSL is no longer secure
- Most **Virtual Private Networks (VPN)** use either TLS or IPsec
- IPsec uses **Authentication Headers (AH)** to provide **authentication**, **integrity** and nonrepudiation and Encapsulating Security Payload (ESP) to provide confidentiality
- **Security baselines**, such as NIST SP 800-53, provide a standardized set of controls that an organization may use as a benchmark
- Deviations from the baseline should be investigated and documented

Quick Recap: Cloud Security Operations

- Documentation is very important in order to get full benefits of system baseline
- Always keep secure copy of secure system baseline
- Baseline should be configured as per vendor recommendations
- **Secondary risk** is any risk resulting from enacting a control/countermeasure to the original risk.

Quick Recap: Cloud Security Operations

- **Multitenancy** complicates performance and capacity monitoring in the cloud. Customers have access to resource monitoring and should pay particular attention to:
  - CPU utilization, Memory utilization, Network bandwidth consumption, Response time

- **Underprovisioned services** exist when demand exceeds capacity. In those cases, services should be upsized to meet changing demand.

- **Overprovisioned services** exist when capacity exceeds demand. Those services should be downsized to reduce costs. Automated alerts notify administrators of monitoring irregularities
- **Capacity management** is concerned with ensuring that sufficient resources are available to meet the needs of cloud customers throughout the environment

Quick Recap: Cloud Security Operations

- **Problem Management** is focused on preventing issues from occurring within a system or process in a proactive manner
- **Incident Management** is focused on the response and mitigation of problems or incidents after they have occurred in a reactionary manner
- **Continuity Management** is focused on the resiliency or restoration or services after an unexpected outage or event
- **Availability Management** is focused on meeting SLA requirements for performance and availability of systems

Quick Recap: Cloud Security Operations

- **Cybersecurity incident response** efforts follow this process
  - Detection -> Response -> Mitigation -> Reporting -> Recovery -> Remediation -> Lessons Learned
- **Network discovery scanning** uses tools like nmap to check for active systems and open ports
- **Network vulnerability scanning** first discovers active services on the network and then probes those services for known vulnerabilities.
- **Web application vulnerability scans** use tools that specialize in probing for web application weaknesses
- The vulnerability management workflow includes three basic steps: **detection, remediation,** and **validation**
- **Penetration testing** goes beyond vulnerability scanning and attempts to exploit vulnerabilities

Quick Recap: Cloud Security Operations

- Security professionals are often called upon to participate in a variety of investigations:
  - **Criminal investigations** look into the violation of a criminal law and use the beyond a reasonable doubt standard of proof
  - **Civil investigations** examine potential violations of civil law and use the preponderance of the evidence standard
  - **Regulatory investigations** examine the violation of a private or public regulatory standard
  - **Administrative investigations** are internal to an organization, supporting administrative activities
- **Investigations** may use several different types of evidence:

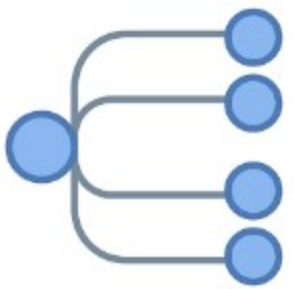
  - **Real evidence** consists of tangible objects that may be brought into court
  - **Documentary evidence** consists of records and other written items and must be authenticated by testimony
  - **Testimonial evidence** is evidence given by a witness, either verbally or in writing

Quick Recap: Cloud Security Operations

- **DNSSEC**
  - Is a security extension to the regular DNS protocol
  - Ensures the integrity of DNS resolutions, but not the confidentiality or availability of them.
  - Is explicitly designed to prove the validity and authenticity of DNS lookups from their authoritative host
  - Provide protection against DNS poisoning
- **Threats** to **DNS infrastructure**: Foot printing, DOS attack, data modification, redirection, spoofing
- **Footprinting** – A process by which an attacker obtains DNS zone data, including DNS domain names, computer names, and IP addresses for sensitive network resources.

Quick Recap: Cloud Security Operations

- **Organizational Normative Framework –** A container for components of an application's security, best practices, catalogued and leveraged by the organization
- **Application Normative Framework –** is a subset of Organizational Normative Framework (ONF)



- **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.
- **Tightly Coupled –** Nodes work together to increase performance

- **Loosely Coupled** – Performance and capacity limit

Quick Recap: Cloud Security Operations

- **Guest Breakout –** Guest OS can access hypervisor or the Guest OS
- **VM-escape –** means a user on a virtual machine can 'Escape' from it and take control over the whole hypervisor
- **Snapshot and Image Security –** It contains sensitive information which needs to be protected

- **Sprawl – Loose control** of the amount of content on your image store
- **Virtualization Sprawl –** is a phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where the administrator can no longer manage them effectively

- **Virtualization sprawl** may also be referred to as virtual machine sprawl, VM sprawl or virtual server sprawl. Its management issue of cloud.
- Sprawl in cloud can cause additional financials/cost.

Quick Recap: Cloud Security Operations

- **Instant-On Gaps –** Vulnerabilities exist from when a VM is powered on and when its security rules can be updated. So its better to include network based security and "virtual patching" that inspects traffic for known attacks before it can get to a newly provisioned or newly started VM
- **Encrypt virtual machine images** when not in use.

Quick Recap: Cloud Security Operations

- **ITIL components**
  - Change management
  - Continuity management
  - Information security management
  - Continual service improvement management
  - Incident management
  - Problem management
  - Release management
  - Deployment management
  - Configuration management
  - Service level management
  - Availability management
  - Capacity management

Legal, Risk and Compliance

Domain 6

Quick Recap: Legal, Risk and Compliance

- **Risks** are the combination of a threat and a corresponding vulnerability
- Every organization is responsible for performing its own risk assessment **Quantitative risk assessment** uses the following formulas:
  - **Single Loss Expectancy =** *Asset Value * Exposure Factor*
  - **Annualized Loss Expectancy =** *Annualized RateofOccurence * SLE*
- Responses to a risk include:
  - **Avoid** risk by changing business practices
  - **Mitigate** risk by implementing controls
  - **Accept** risk and continue operations
  - **Transfer** risk through insurance or contract

- When working with cloud vendors, ensure that vendor's security policies and controls execute at least the same degree of care that you would conduct internally.

Quick Recap: Legal, Risk and Compliance

- **Risk ratings** are Minimal, Low, Moderate, High, and Critical
- **Framing –** Allows the organization to articulate the risks that it needs to managed
- **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.
- **GLBA (Gramm-Leach-Bliley Act) –** IS program is critical component. Tied to financial & insurance organizations and privacy of customer information.
- **AICPA** (American Institute of Certified Public Accountants) is tied to SOX Act.

Quick Recap: Legal, Risk and Compliance

- Customers should document their vendor relationships using a variety of agreements:
  - **Service Level Requirements (SLR) –** document specific requirements that a customer has about any aspect of a vendor's service performance
  - **Service Level Agreements (SLA) –** document the SLRs in a written contract
  - **Memorandums of Understanding (MOU) –** used to document relationships in a less formal manner
  - **Business Partnership Agreements (BPA) –** document the parameters of a business partnership
  - **Master Service Agreements (MSA) –** used to create umbrella relationships as per **Statements of Work (SOW)**
  - **Statements of Work (SOW) –** work requirements for a specific project along with its performance and design expectations
  - **Recovery service level (RSL)** measures the percentage of operations that would be recovered during a BCDR situation.

Quick Recap: Legal, Risk and Compliance

- Understand the **overlapping jurisdictions** that apply to a cloud relationship based upon the location of the customer, service provider, and information subjects.
- Organizations should design their privacy programs to follow the Generally **Accepted Privacy Principles (GAPP)**. These principles include:

1. Management
2. Notice
3. Choice and Consent
4. Collection
5. Use, Retention, and Disposal
6. Access
7. Disclosure to Third Parties
8. Security
9. Quality
10. Monitoring and Enforcement

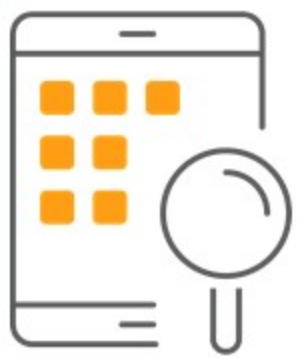
Quick Recap: Legal, Risk and Compliance

- **Due care** is taking reasonable steps to protect the interest of the organization.
- **Due diligence** ensures those steps are carried out.
- **D**ue **D**iligence = **D**o **D**etect
  Due **C**are = **D**o **C**orrect
- Security governance is carried out through
  - **Policies –** high-level objectives (mandatory compliance).
  - **Standards –** detailed technical requirements (mandatory compliance).
  - **Procedures –**step-by-step processes (mandatory compliance).
  - **Guidelines –**offer advice and best practices (optional compliance).

Quick Recap: Legal, Risk and Compliance

- Organizations are subject to a wide variety of legal and regulatory compliance obligations from:
  - **Criminal laws –** that may involve prison or fines
  - **Civil laws –** regulate non-criminal disputes
  - **Administrative laws –** set by government agencies.
  - **Regulations –** from industry bodies

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



Quick Recap: Legal, Risk and Compliance

- **Litigation holds** should be sent as soon as an organization reasonably anticipates litigation.
- Collection should occur when directed by the legal team. Production turns records over to the opposing side. All of these activities are part of the eDiscovery process.

Law/Regulation	Scope
HIPAA/HITECH	Health information
FERPA	Educational records
GLBA	Financial services sector
COPPA	Information related to children under the age of 13
Privacy Act of 1974	Information held by federal agencies
GDPR	PII of European Union residents
PIPEDA	PII of Canadian residents
APEC CPEA	PII of residents of Asian-Pacific nations
SOX	Publicly-traded companies
PCI DSS	Credit and debit card records
NERC CIP	Critical infrastructure

Quick Recap: Legal, Risk and Compliance

- In IaaS, cloud provider has full administrative and system access to everything, they are responsible for forensic data collection within the environment

- In eDiscovery, determining all of the applicable data and locating it for collection and preservation is biggest challenge.
- With multitenancy, eDiscovery becomes more complicated
- **Contractual PII –** When an organization share PII to either CSP or outsource (call centers), they should include in the contract about the adherence of compliance in protecting the PII

- **Regulated PII –** Must adhere to the law and statutory requirements
- **Mandatory breach reporting** is the best example of a key component of regulated PII.

Quick Recap: Legal, Risk and Compliance

- **The SOC 1 Types 1 and 2** are about financial reporting
- **SOC 2** – auditing reports are built on a set of **five principles**: *Security*, *Availability*, *Processing Integrity*, *Confidentiality*, and *Privacy*
- **SOC 3 –** General Use and Public, It is a kind of SSAE audit report that a cloud customer most likely to receive from a cloud provider
- The **SOC 3 is** the least detailed, so the provider is not concerned about revealing it. SOC 3 is only an attestation by the auditor
- The **SOC 2 Type 2** is much more detailed and will most likely be kept closely held by the provider
- An **SOC Type I** report is designed around a specific point in time
- An **SOC Type II** report is designed around a period of time

Quick Recap: Legal, Risk and Compliance

- **Security tests verify** that a control is functioning properly
- **Security assessments** are comprehensive reviews of the security of a system, application, or other tested environment.
- **Auditing –** Define audit objectives, then audit scope, conduct audit, and refine audit/lessons learned

- **Security audits** use testing and assessment techniques but are performed by independent auditors. There are **three types** of security audits:
  - **Internal audits** are performed by an organization's internal audit staff, normally led by a Chief Audit Executive who reports directly to the CEO
  - **External audits** are performed by an outside auditing firm
  - **Third-party audits** are conducted by, or on behalf of, another organization, such as a regulator

Quick Recap: Legal, Risk and Compliance

- Internal audit does not focus on certification, in order to obtain and comply with certifications, independent external audits must be performed and satisfied
- **Virtualization** make it very difficult to perform repeat audits over time to track changes and compliance
- **eDiscovery** pertains to information and data that is in the possession, control, and custody of an organization
- When a cloud service provider receives an eDiscovery order pertaining to one of their customers, the first action they must take is to notify the customer

Quick Recap: Legal, Risk and Compliance

- **State law –** typically refers to the law of each U.S. state (50 states in total, each treated separately), with their own state constitutions, state governments, and state courts
- **Doctrine of Proper Law –** is used when a dispute occurs over which jurisdiction will hear a case
- **Tort law –** refers to civil liability suits
- **Restatement of Law –** Uses relevant factors of applicable law
- **Common law –** refers to laws regarding marriage
- **Criminal law –** refers to violations of state or federal criminal code
- **Privacy law –** Defined as the right of an individual to determine when, how, and to what extent she will release personal information

Best of Luck for your exam.

Thanks!

Questions and Answers

Contact Me

https://www.linkedin.com/in/mahmad1983

Cell/WhatsApp: +92 3111-124-623

Email: mahmad83@gmail.com

For Training, please contact below

CCSP | CISSP | CISM | CISA | CRISC | CGEIT

Contact Me

https://www.linkedin.com/in/mahmad1983

Cell/WhatsApp: +92 3111-124-623

Email: mahmad83@gmail.com