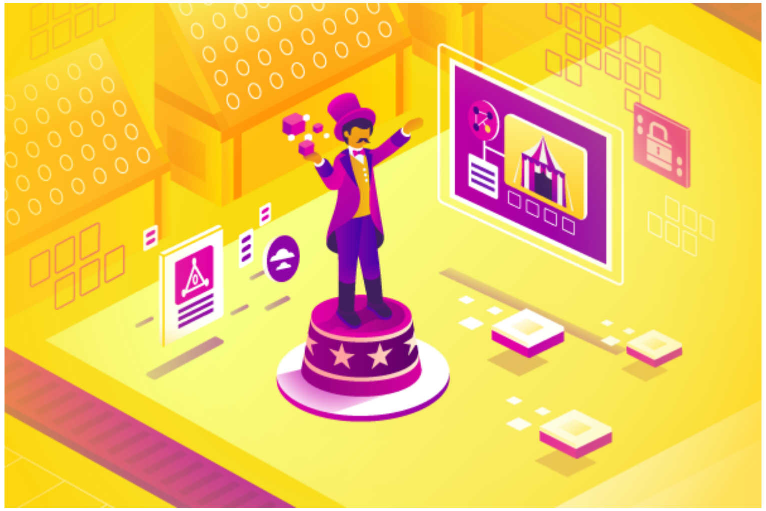


Certified Cloud Security Professional (CCSP)

Study Guide

Bob Salmans
bob.salmans@linuxacademy.com
September 2019

Linux Academy

Contents

Domain 1: Cloud Concepts, Architecture and Design

General Security and Business Philosophy

- **The business drives security. Security does not drive the business:**
  - IT supports the business and its goals.
  - Security hinders a business's efficiency.
  - Business needs drive security, security does not drive the business.

    Ex.: If a business wants to process credit cards and manage cardholder data, it must become PCI compliant. It doesn't make sense for a business that doesn't handle cardholder data to spend money on becoming PCI compliant just because someone in IT feels it would be a good idea.
- **Information security professionals need to understand how the business operates in order to be more effective at their role:**
  - If IT wants to deploy geo-blocking technologies, they can't simply block traffic from all countries. IT must understand how the business works and who they work with before deploying security technologies, or they will hinder the business's progress.
  - IT cannot provide advanced audit capabilities for sensitive data if they don't take the time to communicate with data owners to identify what data is sensitive and where it resides.
- **Functional requirements: Services required for a person of the business to accomplish their job:**
  - Ex.: Sales cannot effectively communicate with customers unless they have remote access to email.

- **Nonfunctional requirements: Services not required for a person of the business to accomplish their job:**
  - Ex.: Sales cannot effectively communicate with customers unless they have remote access to *encrypted* email.
  - Understand the difference between functional and non-functional requirements.
  - Jane needs reliable transportation to her job: Jane needs a car. (Functional)
  - Jane needs reliable transportation to her job: Jane needs a stretch limousine and driver. (Non-functional)
- **CapEx:**
  - Capital expenditure (CapEx) is an upfront investment of a sum of money into a business requirement, such as a building, server farm, network environment, or network operations center (NOC).
- **OpEx:**
  - An OpEx is an operational expenditure where you are paying for a service on a schedule. An example of this would be a building lease or utilities. However, this applies to services as well, such cloud services or hosting services.
- **CapEx vs. OpEx:**
  - Businesses may not have large amounts of capital at their disposal, so instead of building out an on-premises compute solution that could cost large amounts of money, they may instead look into a cloud solution. If the business stands up their compute needs in the cloud, they are paying month to month on only what is needed. Whereas, if they built out their on-premises solution, they would have to invest large amounts of capital upfront and then pay for ongoing costs, such as electricity, warranties, support contracts, and eventually replacement.

A. Cloud Computing Concepts

A1. Cloud Computing Definitions

- **Anything as a Service (XaaS)**: The understanding that there is a vast amount of services available across the internet so you don't need to stand up an on-premises solution.
- **Apache CloudStack**: An open-source cloud computing software for creating, managing, and deploying infrastructure cloud services. A management layer for managing hypervisors and their abilities.

- **Business Continuity (BC)**: The capability of a business to continue delivery of services or products to its customers following a loss of service. Focuses on how the business will continue to serve customers during the incident, not how it will get IT back up and running, which is the focus of disaster recovery (DR).
- **Business Continuity Management**: Management process that builds a framework based on potential threats and their impact on business operations. This framework provides resilience to the business and safeguards the interests of key stakeholders.
- **Cloud app**: A cloud application accessed across the internet, not installed locally.
- **Cloud Application Management Platform (CAMP)**: A specification designed to ease management of applications across public and private cloud platforms.
- **Cloud computing**: A type of computing that shares computing resources of remote environments to accomplish work, instead of using local servers.
- **Cloud database**: A database accessible to clients across the internet. Also refers to Database as a Service (DBaaS). These cloud databases use cloud computing to achieve optimization, scaling, high availability, and multi-tenancy.
- **Cloud enablement**: Making cloud services available to a client.
- **Cloud management**: Software and technology used to monitor and operate cloud environments. These tools help ensure cloud resources are working optimally.
- **Cloud OS**: A phrase used in place of Platform as a Service (PaaS) to identify an association with cloud computing.
- **Cloud portability**: The ability to move applications and data between different cloud service providers (CSPs) or between public and private cloud environments.
- **Cloud provisioning**: The deployment of cloud services to meet a need.
- **Cloud service provider (CSP)**: Company providing cloud services to customers.
- **Desktop as a Service (DaaS)**: A virtual desktop infrastructure (VDI), also called a hosted desktop service. Simply a desktop in the cloud you connect to and use with applications installed on it.
- **Enterprise application**: Applications or software used by large organizations. Generally refers to large-scale applications not suited for small business or individual needs.

- **Eucalyptus**: Open-source cloud computing and IaaS platform for enabling AWS-compatible private and hybrid clouds.
- **Event**: A change of state that has significance for the management of an IT service. Sometimes referred to as an alert or notification.
- **Hybrid cloud storage**: A combination of public and private cloud storage. Sensitive data will reside in the private cloud, while other data or applications may reside in the public cloud.
- **Infrastructure as a Service (IaaS)**: A computer infrastructure being delivered as a service. This includes compute, storage, network, and internet access. Simply a fully functional virtual environment on which customers provision virtual hosts.
- **Managed service provider (MSP)**: Managed service providers (MSPs) provide various IT services to customers such as monitoring, patching, help desk, and network operations center.
- **Mean time between failures (MTBF)**: Measure of the average time between failures of a component or system.
- **Mean time to repair (MTTR)**: Measure of the average time it should take to repair a component or system failure.
- **Mobile cloud storage**: Cloud storage used to store a customer's mobile device data in the cloud providing access from anywhere.
- **Multi-tenant**: Having multiple customers using the same public cloud. Data is logically separated by security controls but still runs on the same shared underlying hardware.
- **On-demand services**: Service model allowing customers to scale their consumed resources without assistance from the provider in real time.
- **Platform as a Service (PaaS)**: A cloud-based platform on which clients deploy their applications. The CSP will manage all underlying infrastructure, including operating system, compute hardware, and network. The customer is only responsible for managing their application code.
- **Private cloud**: Also known as internal or corporate cloud, this cloud compute platform is protected by the corporate firewall under the control of the IT department, not a CSP. Allows the IT department to control the security of the data and meet regulatory compliance. May be a corporate-owned data center referred to as a corporate cloud or can also be provided by a CSP offering isolated cloud services.

- **Public cloud storage**: Cloud storage in which the enterprise and storage services provider are separate and the data is stored outside the enterprise data center.
- **Recovery point objective (RPO)**: Helps determine how much information must be restored from backups after an event. "How much data is the company willing to lose?"
- **Recovery time objective (RTO)**: How fast you need individual systems to be back up and running after a disaster or critical failure, generally measured in hours. For example, the RTO for a business-critical application may be four hours.
- **Scalability**: The ability to increase resources to meet demand in near real time.
- **Software as a Service (SaaS)**: Cloud-based software offered to clients accessed across the internet, most often as a web-based service. Think web-based applications you log in to and use.
- **Vertical cloud computing**: The optimization of cloud computing and services for a specific industry. An example would be cloud resources for the entertainment industry, which may have GPUs available to increase compute power for rendering of images and video.

A2. Cloud Computing Roles

- **Cloud customer**: An individual or organization that uses cloud-based services.
- **Cloud service auditor**: A third party that verifies CSPs are meeting service-level agreements (SLAs).
- **Cloud service brokerage (CSB)**: Organization that looks to add value to cloud services through relationships with multiple CSPs. They are used to help customers identify the best cloud solution for them. CSBs sometimes resell cloud services.
- **Cloud service provider**: Company providing cloud services to customers.
- **Cloud service partner**: Includes other roles, such as cloud service auditor and cloud service broker.

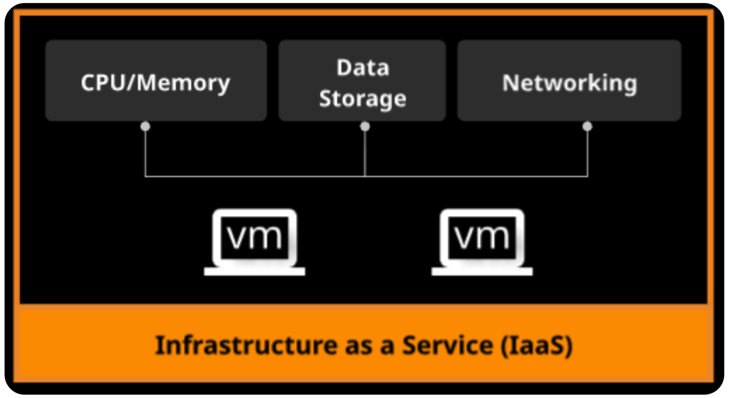
A3. Key Cloud Computing Characteristics

- **On-demand self-service**: The ability for cloud service customers to provision new cloud services or increase existing services on demand. This can be dangerous, as these services don't require approval from finance or another process — they simply require access to a management console and a few button clicks.
- **Broad network access**: You should never experience network bottlenecks due to use of technologies such as routing, load balancers, multiple sites, etc.
- **Resourcing pool**: Provider owns a large pool of resources (compute, storage, network, etc.), and customers each get an amount of these "pooled" resources. By having a "pool," the vast majority of these resources are shared and not dedicated. This means the provider can spend less money on resources as they are getting more use out of each resource as opposed to dedicated physical servers.
- **Elasticity**: The ability to scale back resources as needed so you are not paying for unused resources.
- **Metered or measured service**: Customer is charged only for what resources they use. Also allows for organizations to charge individual departments within the organization for resources used by that department.

A4. Building Block Technologies

IaaS Building Blocks:

- **CSPs**: Provide CPU, memory, storage, networking, and overall virtualization technology
- **Customer**: Provide the OSes, middleware, and applications



B. Describe Cloud Reference Architecture

B1. Cloud Computing Activities

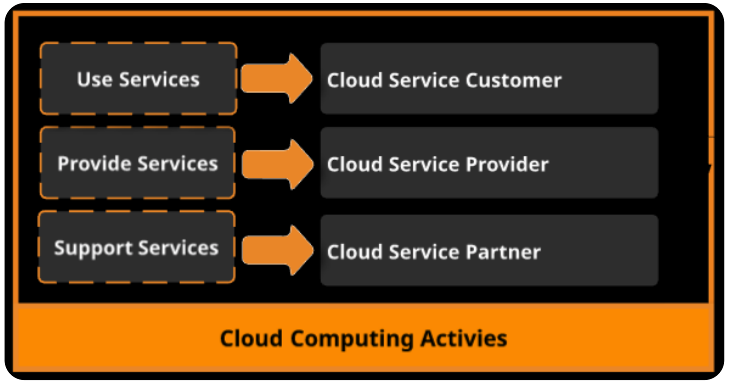
Activities can be organized into three groups:

- **Activities that use services (cloud service customer)**
    - Use cloud services (create accounts and resources)
    - Perform a trial (proof of concept)
    - Monitor service (validate SLAs, bill internal departments)
    - Administer service security (manage policies, organize data, audit)
    - Provide billing and usage reports
    - Handle problems (assess impact, troubleshoot, remedy)
    - Performing business administration (handle billing invoices, account relation)
    - Select and purchase services
- **Activities that provide services (cloud service provider)**
    - Cloud operations manager (prepare systems, monitor/manage services)
    - Cloud services deployment manager (define processes, gather metrics)
    - Cloud service manager (provide services, service-level management)
    - Cloud service business manager (manage business plan, customer relations, financial processing)
    - Cloud support and care representative (handle customer requests)
    - Inter-cloud provider (manage peer cloud services, perform peering and federation)
    - Cloud service security and risk manager (manage security and risks, design and implement service continuity, ensure compliance)
    - Network provider (provide network connectivity and service, network management)

- **Activities that support services (cloud service partners):**
  - Cloud service developer (design, create and maintain service components, compose and test services)
  - Cloud auditor (perform audits, report results)
  - Cloud service broker (acquire and assess customers, asses marketplace, create legal agreements)

B2. Cloud Service Capabilities

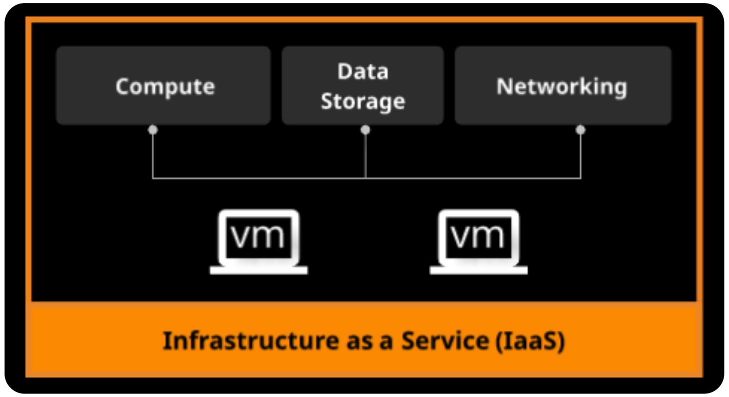
Cloud services are broken down into three capabilities:



- **Application capability**
  - The cloud service customer uses the cloud service provider's applications.
- **Infrastructure capability**
  - The cloud service customer can provision and use processing, storage, or networking resources.
- **Platform capability**
  - The cloud service customer can deploy, manage, and run their own applications using one or more programming languages and one or more execution environments supported by the CSP.

B3. Cloud Service Categories

Infrastructure as a Service (IaaS)



- **The cloud service customer can provision and use processing, storage, or networking resources.**
- **Key components and characteristics:**
  - Scale
  - Converged network and IT capacity pool
  - Self-service and on-demand capacity
  - High reliability and resilience
- **Key benefits:**
  - Measured/metered use
  - Scalability
  - Reduced Total Cost of Ownership (TCO)

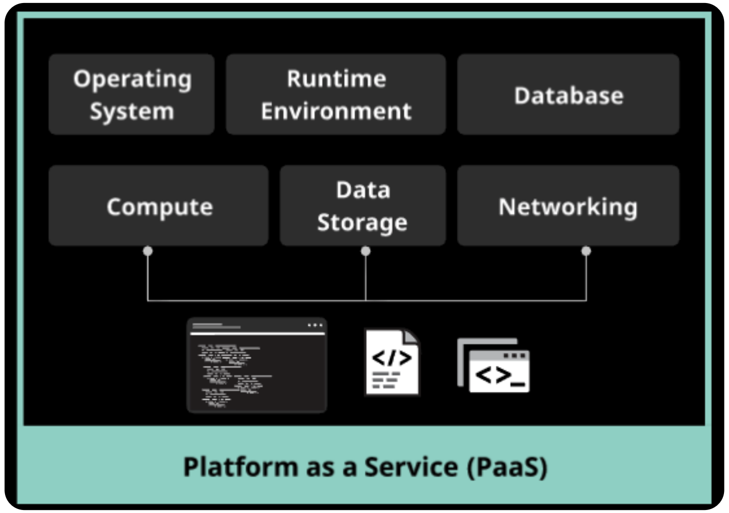
    No replacement costs

    No maintenance fees

    No cooling and power requirements

    No upfront hardware and licensing purchases (CapEx)
  - Reduced energy and cooling costs

Platform as a Service (PaaS)



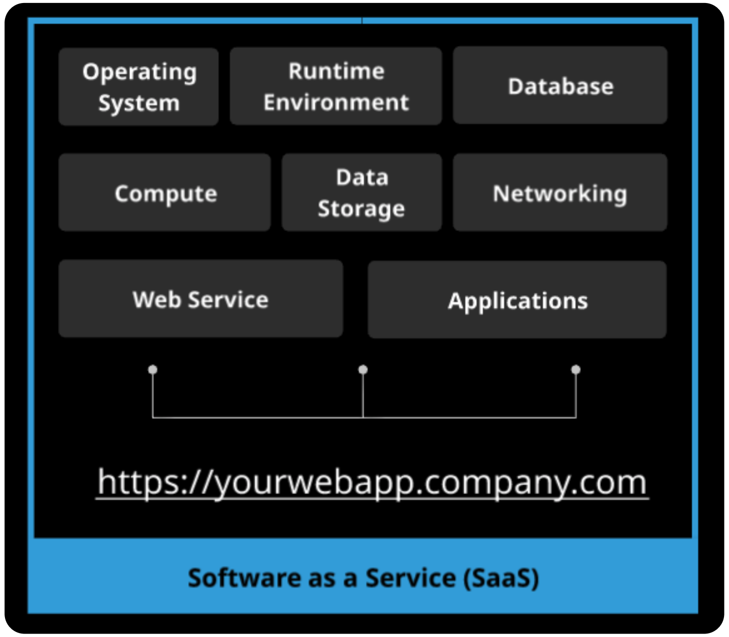
The cloud service customer can deploy, manage, and run their own applications using one or more programming languages and one or more execution environments supported by the CSP.

- **Key capabilities and characteristics:**
  - Supports multiple languages and frameworks
  - Multiple hosting environments

    Public cloud, private cloud, hybrid, bare metal, etc.
  - Flexibility
  - Allow choice and reduce lock-in

    Back to flexibility and allowing programmers to create as they see fit
  - Ability to auto-scale
- **Key benefits:**
  - Operating systems can be changed and upgraded frequently
  - Global collaboration
  - Services made available globally via the cloud, technology isn't crossing borders — users are
  - Cost reduction — single vendor can meet all the needs allowing for savings

Software as a Service (SaaS)



The cloud service customer uses the cloud service provider's applications.

- **SaaS delivery models:**
  - Hosted application management (hosted AM)
    - Provider hosts commercially available software available across the internet
      - Webmail
      - Accounting apps
      - HR apps
    - Software on demand
      - CSP gives network-based access to a single copy of an application that was set up specifically for SaaS distribution.
      - Dedicated instance for customer
      - Scales as needed, which means licenses also scale
- **SaaS benefits:**
  - Cost reduction
    - No hardware to purchase or upgrade
    - No support contracts for hardware
  - Application/software licensing
    - No need to purchase licenses and support up front
    - Licenses are leased as part of the service

Moved from CapEx to OpEx

- Reduced support cost

  No support contracts to purchase

  Support is handled by the CSP

- **Key benefits of SaaS:**
  - Ease of use and limited administration

    Requires less labor to manage
  - Automatic updates and patch management of underlying infrastructure as it's handled by the CSP
  - Standardization

    All users work on the same platform in the cloud so it's standardized
  - Global access

Communications as a Service (CaaS)

Provides the cloud service customer real-time interaction and collaboration

Compute as a Service (CompaaS)

Provides cloud service customers the ability to provision and use processing resources needed to deploy and run software

Data Storage as a Service (DSaaS)

Provides cloud service customers the ability to provision and use data storage and related capabilities

Network as a Service (NaaS)

Provides cloud service customers the ability to use transport connectivity and related network capabilities

B4. Cloud Deployment Models

Four main types of deployment models:

- Public
- Private
- Hybrid
- Community

The cloud deployment model you select will be based on:

- Risk appetite
- Cost
- Compliance and regulatory requirements
- Legal obligations
- Business strategy

Public Cloud Model

Definition according to NIST:

> *"The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."*

Key: Anyone can sign up with the cloud provider and use the resources.

Public Cloud Benefits:

- Easy and inexpensive to set up (provider has paid for the upfront startup costs)
- Easy to use
- Scalable
- Pay as you go, no wasted resources

Private Cloud Model

Definition according to NIST:

> *"The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."*

Key: Provisioned for use by a single organization

Private cloud benefits:

- Increased control over data, underlying systems, and applications
- Ownership and retention of governance controls
- Assurance of data location, which simplifies legal and compliance requirements

These are most often used in large environments with compliance or regulatory requirements.

Hybrid Cloud Model

Definition according to NIST:

> *"The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."*

Key: Composition or combination of two or more cloud infrastructures

Key benefits:

- Ability to retain ownership and management of critical tasks and processes
- Reuse technology already owned
- Control critical business components
- Cost-effective by using public cloud for non-critical/non-compliance functions
- Use cloud bursting and disaster recovery functions of the cloud

Community Cloud Model

Definition according to NIST:

> *"The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."*

Key: Provisioned for exclusive use by a specific community of consumers. A group of like-minded organizations build out their own cloud and share the cost.

Example: A group of doctors' offices come together to create a cloud solution that hosts their electronic medical records (EMR) application. They all can access and use the EMR, and they share the costs associated with the cloud resources.

Key benefits:

- Flexibility and scalability
- High availability and reliability
- Secure and compliant
- Improved services
- Reduced cost (shared costs)

B5. Cloud Shared Considerations

- **Auditability**: The capability of collecting and making available necessary evidential information related to the operation and use of a cloud service for the purpose of conducting an audit.
    - What logs are available to the customer without needing to request special access?
    - What additional charges may be incurred for log access?
- **Availability**: The state of being accessible and usable on demand by an authorized user.
- **Governance**: The system by which the provision and use of cloud services is directed and controlled.
- **Interoperability**: The ability of a cloud service customer to interact with cloud services in a predictable manner, or the ability for one cloud service to interact with another cloud service.
- **Maintenance**: Maintenance and upgrades can change the way services function, therefore it's important that maintenance of services be subject to governance practices that are transparent to the customer.
    - Notification of maintenance windows and scheduled upgrades
    - Disclosure of roll-back practices
    - SLA should document maintenance practices
- **Versioning**: Labeling of a service's version for easy identification of the version. If significant changes are being made, both the old and new version should be offered in parallel to reduce impact to customers if there is an issue with the new version.
- **Performance**: The cloud services meeting the metrics defined in the SLA. These metrics include availability, response time, latency, data throughput, etc.
- **Portability**: The ability for a cloud service customer to easily migrate their data between cloud service providers. This is a key factor to consider when considering a cloud service provider.
- **Protection of personally identifiable information (PII)**: Cloud service providers "should" protect PII. This is something to look for in SLAs.
- **Resiliency**: The ability of a system to provide and maintain an acceptable level of service during a system fault. This is where monitoring and high availability come into play.

- **Reversability**: This goes two ways. The first is the ability for a cloud service provider to recover cloud service customer data and application artifacts in the event of deletion. The second is the ability of a cloud service provider to delete all cloud service customer data after an agreed-upon date (right to be forgotten).
- **Security**: This includes many capabilities, such as access control, confidentiality, integrity, and availability (CIA triad). This also includes management and administrative functions.
- **Service-level agreement (SLA)**: Representing measurable elements needed to ensure an agreed-upon quality of service between the cloud service customer and provider. The key is "measurable." The SLA should specify information related to the availability, confidentiality, and integrity of the services provided.

B6. Impact of Related Technologies

- **Machine learning (ML) and artificial intelligence (AI)**: Using pattern recognition and computational learning to make predictions
    - Many cloud vendors are now offering ML and AI as a service.
    - Cloud vendors have the resources to build out environments suited for this type of data analysis.
- **Blockchain**: A protocol that uses a decentralized framework to maintain integrity within the data
    - Cloud was originally the offloading of service from on-premises to a cloud vendor's premises where customers use resources from one or more data centers.
    - Blockchain could be used to manage globally distributed workloads between data centers so that the data resides in multiple data centers at once.
    - Not only would this allow for a new type of decentralized cloud, but it would also be used to guarantee integrity of the data.
- **Internet of Things (IoT)**: IoT devices are generally sensors or other simple devices with simplified tasks. The "internet" of IoT indicates these devices are internet-connected and upload data to a destination somewhere online.
    - Many cloud vendors offer IoT services, including creating images for individual devices, cloud-based data analysis, and the integration of AI.

- **Containers**: Containers are small packages of code that include an application, its dependencies, and libraries. That's it! It then uses the underlying container operating system on which it runs for other services, such as networking. Containers are like a stripped-down version of virtualized virtual machines (VMs).
    - Containers are very small and generally require very little resources, hence they start up very quickly and cost very little to run. A great alternative to a full-blown VM instance.
    - They can scale very quickly.
    - They are designed to do only a single job, such as a web service that allows you to separate each service into its own container. This increases resiliency and security.
- **Quantum computing**: Quantum computing gets its massive compute power by tapping into quantum physics and not the use of micro-transistors. Traditional computing uses the values of 0 and 1 in bits, but quantum computing can store multiple values in qubits.
    - Vendors such as Rigetti, Google, IBM, and Microsoft have made quantum CPUs, but they are still in the infancy of the projects and are working to build applications that can take advantage of the processing power so they can measure the processing power.
    - Eventually, cloud service providers will offer quantum computing services to their customers. We can only imagine that with the shared resource framework, providers will be able to offer quantum computing services at a much more affordable rate than attempting to purchase a quantum computing server.

C. Understand Security Concepts Relevant to Cloud Computing

C1. Cryptography and Key Management

Confidentiality: Controlling authorized access to data in order to protect the privacy of the data

Data in Transit (Data in Motion)

- **Data crosses untrusted networks**
  - Across the internet
  - Between cloud providers
  - Any network you don't have 100% control over
- **SSL and TLS**
  - Secure Sockets Layer (SSL) uses private and public keys to encrypt data over the internet.
  - Transport Layer Security (TLS) provides a transport layer (OSI model) encrypted tunnel between applications. Often used with mail services.
- **IPSec**
  - Used in network-to-network VPN tunnels

    Tunnel mode encapsulates the entire original packet
  - Uses cryptography algorithms such as 3DES and AES

Data at Rest

- Data not in use by users or applications
- Be aware encryption can impact performance and testing should be done
- Not required for all data — only data deemed sensitive (PII, PCI, HIPAA, IP)
    - Personally identifiable information (PII)
    - Payment Card Industry (PCI)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Intellectual property (IP)
- Reduces risk of unauthorized data access
- In some cases can make it hard to retrieve data
    - Lost keys in some cases
    - Dispute with the CSP
    - Just something to keep in mind

Key Management

- **Separation of duties is super important**
    - Key managers should be separate from providers
    - Keys kept on-premises in an isolated secure location
- **Approaches for cloud computing key management**
    - *Remote Key Management Service (KMS)*: Customer maintains the KMS on-premises. Connectivity is required between the KMS server and the cloud data for encryption/decryption of data.

    - *Client-Side Key Management*: CSP provides the KMS, but it resides on customer premises. Then customer generates keys, encrypts data, and uploads to the cloud.

C2. Access Control

Access control has evolved to work with other services such as single sign-on (SSO), multi-factor authentication (MFA), and other authentication and authorization services, and is now generally known as identity and access management (IAM).

IAM works with people, processes, and systems to control access to resources.

- Validate identity
- Grant level of access to data, services, applications, etc.
- Generally uses a minimum of two factors of authentication to validate a user's identity.

IAM Key Phases

- **Provisioning and deprovisioning user accounts**
    - Deprovisioning is a risk mitigation technique (house cleaning)
    - Deprovision individual permissions due to role change
- **Centralized directory services**
    - Stores, processes, and maintains a repository, including unique IDs and locations
    - Primary protocol is Lightweight Directory Access Protocol (LDAP), based on the X.500 standard

        LDAP uses a hierarchical data structure

        Privileged Identity Management (PIM) is an identity management system that includes features such as:

            Managing privileged access

      - Time-bound rules
      - Geo-based rules
      - Audit capabilities
      - Notification capabilities
      - Forcing use of MFA
  - IAM should use features of PIM for administrative access accounts
    - MFA should always be used on administrative accounts
  - Trust and confidence in the accuracy and integrity of the directory service is paramount
- **Privileged user management**
  - Privileged accounts carry the highest risk and impact
  - Key components as it pertains to privileged accounts are:
    - Usage tracking
    - Authentication success and failure tracking
    - Authorization date and times
    - Reporting capabilities
    - Password management (complexity, length, MFA)
  - Requirements should be driven by organizational policies and procedures
- **Authorization and access management**
  - Authorization determines a user's right to access a resource
  - Access management is the process of providing access to resources once a user is authorized to access it.

C3. Data and Media Sanitization

- **The ability to remove all data from a system is critical to ensuring confidentiality in the cloud. We can't have data remnants remaining for someone else to find at a later point.**
- **If a vendor is not in compliance with standards requiring the provider to have a solution for securely removing data, how can we ensure it's actually being wiped?**
  - Cryptographic erasure: Erase, overwrite with pattern, erase again
  - Data overwriting: Simply overwriting data may be sufficient for some data but not sensitive data (PII, PCI, HIPAA, IP)
  - Remember: Deleting files only makes them invisible to the user; the files are still there until overwritten by the operating system with other data.
  - Key destruction of an encryption key is not sufficient, as the key could be recovered forensically and used to access data that has not been wiped properly.

> Other than degaussing media or complete physical destruction, an attacker who has enough resources and time can access data that has been written over and erased several times. These types of destruction are merely a deterrent.

C4. Network Security

The perimeter of a CSP can be hard to identify as it may simply be a carrier's trunk into a building or it could be a series of micro instances running as load balancers.

VM Attacks

Once a VM is compromised, the attacker has access to the shared services of that VM.

Hypervisor Attacks

- **Hypervisors are a great target because they provide control over hosted VMs and access to shared resources.**
- **Common hypervisor attacks are known as hyperjacking in which an attacker will hijack a hypervisor using a Virtual Machine Monitor (VMM) such as:**
  - SubVirt
  - Blue Pill: Hypervisor rootkit using AMD Secure Virtual Machine (SVM)
  - Vitriol: Hypervisor rootkit using Intel VT-x
  - Direct Kernel Structure Manipulation (DKSM)
- **VM Escape is another type of attack in which the attacker crashed the guest OS of a VM in order to run attack code that allows them to take control of the hypervisor host.**

Virtual Switch Attacks

- **Virtual switches are vulnerable to some of the same attacks as physical switches, such as:**
  - VLAN hopping
  - ARP table overflow
  - ARP poisoning

Network Security Groups

- Access lists permitting or denying traffic
- Can be assigned at the VM level

- Can be assigned at the network/subnet level

C5. Virtualization Security

The *hypervisor* allows multiple operating systems to share a single hardware host. The hypervisor is the single most critical component in virtualization.

Types of hypervisors:

- **Type 1 hypervisor:** Bare metal hypervisors that run directly on the hardware using a hypervisor operating system (e.g., VMware ESXi and Citrix XenServer)
    - Relate to hardware security
    - Has a reduced attack surface compared to Type 2 hypervisors
    - Vendor controls all software on the hypervisor OS
    - Increased reliability and robustness over Type 2 hypervisors due to closed environment
- **Type 2 hypervisor:** Run on a host OS and provide virtualization services (e.g., VMware Workstation and Virtual Box)
    - Relates to OS security
    - More attractive to attackers because they can use vulnerabilities of the host OS and any other applications installed on the machine

C6. Common Threats

Data Breaches

- **Cloud computing has widened the scope for data breaches**
  - Multitenancy
  - Shared databases
  - Multiple locations
  - Key management
  - Creates a widely dispersed attack surface and greater opportunity for data breaches
- **Smart devices have increased exponentially**
  - Lost devices
  - Devices are costly and sometimes difficult to properly manage (insecure devices)
- **In the event of a breach, companies with sensitive data may:**
  - Need to publicly disclose the breach (lose credibility)
  - Pay fines
  - Lose the ability to legally process certain types of data

Data Loss

- **The loss of information by deletion, overwriting, corruption, or loss of integrity**
- **Items to consider in the cloud as it pertains to data loss:**
  - Is the provider responsible for backups?
  - If the provider is performing backups, is it all of the data or only a subset?

    - What is the process for restoring data?
    - On a shared platform, such as an application, can a single customer's data be restored?
- **Remember: If you lose an encryption key and can no longer unencrypt and use data, it is considered lost.**

Account or Service Traffic Hijacking

- This type of hijacking is frequently done via social engineering attacks (phishing of some sort).
- Some attacks use sniffing to capture credentials.
- Newer attacks use communications from a compromised third party that is a trusted organization, such as a vendor.
- Awareness is key to thwarting these attacks.
- MFA should be used on all services accessible from the internet.

Insecure Interfaces and APIs

- We use application programming interfaces (APIs) to interact with cloud services.
- These APIs must follow policies.
- All additions to APIs must be scrutinized to validate secure functionality.

Denial of Service

- Denial of Service (DoS) attacks prevent users from being able to access services
- DoS attacks can target:
    - Memory buffers

    - Network bandwidth
    - Processing power
    - And much much more
- Distributed DoS (DDoS) attacks are launched from multiple locations against a single target.
- Need to work to reduce single points of failure to limit effectiveness of DoS attacks.

Malicious Insiders

- Someone intentionally misuses access to data, which affects the confidentiality of that data.
- This someone could be a current or former employee, contractor, or other business partner.

Abuse of Cloud Services

- If willing to pay for resources, attackers can use cloud services for harm, such as:
    - Dictionary attacks
    - DoS attack
    - Password cracking
- CSPs do watch for some of these activities (specifically DoS) and do work to mitigate them.

Insufficient Due Diligence

- Due diligence: The act of investigating and understanding the risks a company faces
- Due care: The development and implementation of policies and procedures to aid in protecting the company from threats

- As a cloud security professional, you should consider:
  - Security practices of a CSP
  - If your CSP was to close its doors, are you poised to quickly change CSPs?
  - Always have a backup plan (exit strategy)

Shared Technology Vulnerabilities

As cloud is often a shared environment, meaning underlying hardware and technologies are shared, any vulnerabilities that reside in that hardware or technology is also shared.

Cloud providers should use a defense-in-depth strategy and implement controls for each layer:

- Compute
- Storage
- Network
- Application
- User security enforcement
- Monitoring

D. Understand Design Principles of Secure Cloud Computing

D1. Cloud Secure Data Lifecycle

Data is the most valuable asset for most organizations.

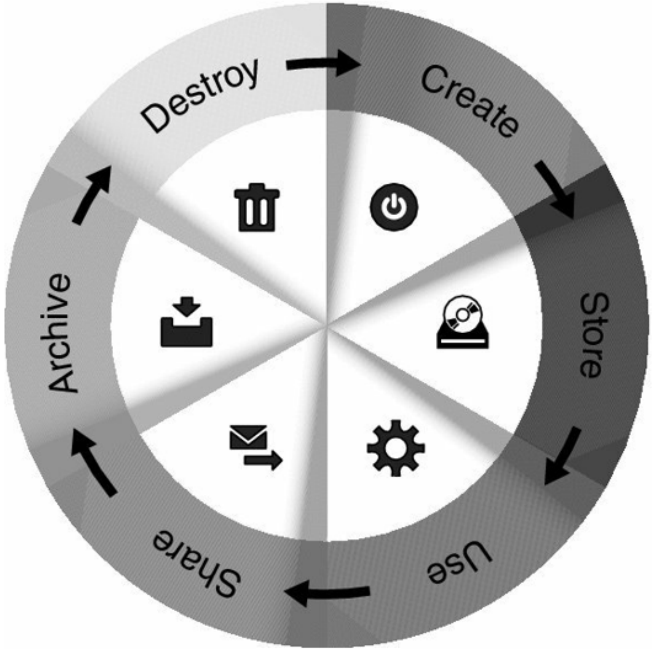
Data should be managed across a lifecycle that includes the following six phases:

1. Create
2. Store
3. Use
4. Share
5. Archive
6. Destroy

It is very important to *always* know where data resides and who is accessing it.

Data governance terms to be familiar with:

- **Information classification:** Description of valuable data categories (confidential, regulated, etc.)
- **Information management policies:** What activities are allowed for different information classifications (cannot leave premise, cannot be copied to external media, etc.)
- **Location and jurisdictional policies:** Where can data be geographically located and any regulatory or legal concerns
- **Authorizations:** Who is permitted to access different types of data
- **Custodianship:** Who is responsible for managing specific data



D2. Cloud based Disaster Recovery (DR) and Business Continuity (BC) planning

- ***Business Continuity Management (BCM)*: The process of reviewing threats and risks to an organization as part of the risk management process**
  - The *goal* of BCM is to keep the business operational during a disruption.
  - BCM should occur annually or biannually.
- ***Disaster Recovery Planning (DRP)*: The process of creating plans to execute in the event of a disaster**
  - The *goal* of DRP is to quickly reestablish the affected areas of the business.
  - Not all services are equal.

    Revenue-centric services will be of more importance.
- **Combines as *Business continuity and disaster recovery (BCDR)***
- **Critical success factors for business continuity (BC) in the cloud are:**
  - Understand your responsibilities versus the CSP's

    Customer's responsibilities

    CSP's responsibilities

    Interdependencies or third-party vendors such as application vendors

    Order of restoration, what has priority

    Right to audit capabilities to validate capabilities

    Communications of any issues

    Need for backups in a secondary location other than the CSP
  - Document in the SLA what BCDR is handled by CSP and to what degree

    Penalties for loss of service

RTO/RPO

Loss of integrity

Points of contact and escalation process

Failover capabilities

Communication of changes being made

Clearly defined responsibilities

Where third parties are being used by the CSP

- **Cloud customer should be *fully satisfied* with the BCDR details prior to signing any agreements or accepting terms. Once signed, future modifications may result in charges to the customer.**

Important SLA Components

- Undocumented single points of failure should not exist.
- Migration to another CSP should be permitted within an agreed-upon timeframe.
- If alternate CSPs cannot provide necessary services, an on-premises solution may be required.
- Customer should be able to verify data integrity via automated controls.
- Data backup solutions should allow for granular settings.
- Regular reviews of the SLA should occur to ensure cloud services continue to meet the needs of the business.

D3. Cost Benefit Analysis

Cost is almost *always* a key data point in deciding to go to the cloud.

Things to consider pertaining to cost:

- **Resource pooling**: CSPs offer pooled resources that keep cost down, and that savings is passed on to the customers.
- **Shift from CapEx to OpEx**: Why not use a "pay as you go" model instead of a large upfront investment?
- **Factor in time and efficiencies**: Cloud is easy to manage and has much automation built in.
- **Include depreciation**: By using cloud, there is no company owned to depreciate off the books.
- **Reduction in maintenance and configuration time**: CSPs handle a large portion of this.
- **Shift in focus**: Allows for more focus on the business as less labor is required to manage a cloud environment.
- **Utility costs**: No need to pay for added electricity and cooling of on-premises hardware.
- **Software and licensing cost**: CSPs can provide great pricing on licenses as they purchase in bulk, and this cost is often included in the services being purchased.
- **Pay per usage**: Only pay for what you use and the ability to track usage so individual users/departments can be billed internally.

Other things to consider when calculating the total cost of ownership (TCO):

- Legal costs (contract reviews)
- Contract and SLA negotiations
- Required training
- Reporting capabilities
- Audit capabilities

D4. Functional Security Requirements

- **Functional requirements:** Services required for a person or the business to accomplish their job
  - Does cloud meet your functional requirements?
  - Does a specific cloud vendor meet your functional requirements?
- **Vendor Lock-In:** A situation in which a customer may be unable to leave, migrate, or transfer from one CSP to another
  - Contract and SLA review is a *must*.
- **Interoperability:** The ability of a cloud service customer to interact with cloud services in a predictable manner, or the ability for one cloud service to interact with another cloud service
  - Avoid proprietary formats and technology.
  - Regularly review legal and regulatory requirements.
- **Portability:** The ability for a cloud service customer to easily migrate their data between cloud service providers. This is a key factor to consider when considering a cloud service provider.
  - Ensure favorable contract terms for portability.
  - Have an exit strategy from day one.
  - Avoid proprietary formats and technology.

D5. Security Considerations for Different Cloud Categories

- **Security Considerations for IaaS**
  - Controlling network access

    Using security groups to open and close ports

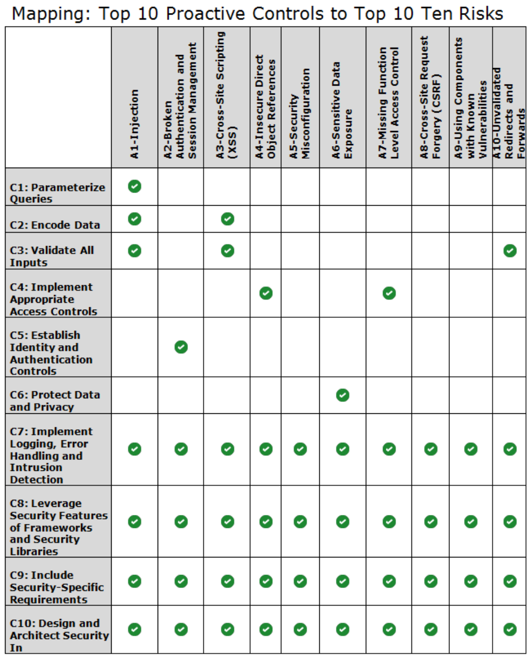
    Configuration of services running on VMs

    Access control within applications

    - Failover or other redundancy
    - Monitoring for availability, security, and audit purposes
    - Patching of applications and VM OSes
- **Security Considerations for SaaS**
    - Access control to applications
        - Secure passwords
        - MFA
        - Account lockout and notifications
        - VPN access requirements
    - Controlling devices where application is installed (BYOD)
    - Monitoring for availability, security, and audit purposes
- **Security Considerations for PaaS**
    - System and resource isolations (due to multitenancy)
    - Access control to applications and permissions
    - Secure coding practices for customer build applications
    - Monitoring for availability, security, and audit purposes
    - Protection against malware
- **For All of These Cloud Categories**
    - Know where your data is
    - Review contracts and SLAs so you know what to expect
        - What your services are
        - What turnaround time for requests are
        - What BCDR services are available and agreed upon

OWASP Top 10: A list of the 10 most common web application security risks

- Great reference document for keeping up with web application vulnerabilities
- Should read through them and understand prevention methods



Mapping: Top 10 Proactive Controls to Top 10 Ten Risks

	A1-Injection	A2-Broken Authentication and Session Management	A3-Cross-Site Scripting (XSS)	A4-Insecure Direct Object References	A5-Security Misconfiguration	A6-Sensitive Data Exposure	A7-Missing Function Level Access Control	A8-Cross-Site Request Forgery (CSRF)	A9-Using Components with Known Vulnerabilities	A10-Unvalidated Redirects and Forwards
C1: Parameterize Queries	✓									
C2: Encode Data	✓		✓							
C3: Validate All Inputs	✓		✓							✓
C4: Implement Appropriate Access Controls				✓			✓			
C5: Establish Identity and Authentication Controls		✓								
C6: Protect Data and Privacy						✓				
C7: Implement Logging, Error Handling and Intrusion Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C8: Leverage Security Features of Frameworks and Security Libraries	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C9: Include Security-Specific Requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C10: Design and Architect Security In	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

E. Evaluate Cloud Service Providers

E1. Verification Against Criteria

Key Thought:

- If it cannot be measured, it cannot be managed.
  - How do you know something is working or is in compliance if you cannot see the data proving it to be true?

How can we evaluate cloud vendors effectively? Surely there's a tool out there to help with this! Well, there are several. Here are the two main tools:

European Union Agency for Cybersecurity (ENISA)**

- **Cloud Certification Schemes List (CCSL):** Provides an overview of different cloud certification schemes (certifications) and shows the main characteristics of each scheme
  - CCSL answers questions such as:

    What are the underlying standards?

    Who issues the certification?

    Is the CSP audited?

    Who performs the audits?

  - CCSL provides information for the following schemes:

    Certified Cloud Service

    CSA Attestation - OCF Level 2

    EuroCloud Star Audit Certification

    ISO/IEC 27001

    PCI-DSS v3

    Service Organization Control (SOC) 1, 2, 3

    Cloud Industry Forum Code of Practice

- **Cloud Certification Schemes Metaframework (CCSM):** An extension of the CCSL designed to provide a high-level mapping of security requirements of the customer to security objectives in existing cloud security schemes.
  - To access this framework and view different schemes you can use the "CCSM Online Procurement Tool," which allows you to select your security objectives and will show which security schemes (certifications) include your objectives. **Here is a link** to that tool.

Cloud Security Alliance

- *CSA Security, Trust, and Assurance Registry (STAR)*: Created in 2011 as there was a need for a single consistent framework by which cloud vendors could be evaluated. STAR is now managed by the Cloud Security Alliance (CSA).

  - There are two parts to STAR:
    1. Cloud Controls Matrix (CCM): A list of security controls and principles for the cloud environment, cross-referenced to other frameworks such as COBIT, ISO, and NIST
    2. Consensus Assessments Initiative Questionnaire (CAIQ): A self-assessment performed by the cloud provider detailing their evaluation of the practice areas and control groups they use in their services

    - There are three levels of STAR certification:
        1. Self-Assessment: Requires release of publication of due diligence assessments against the CSA's questionnaire
        2. CSA STAR Attestation: Requires the release and publication of results of a third-party audit of the cloud vendor against CSA CCM and ISO 27001:2013 requirements or an AICPA SOC 2
        3. Continuous Auditing: Requires the release and publication of results related to the security properties of monitoring based on the CloudTrust Protocol

These tools help us better grasp standards (schemes/certifications) criteria and identify which ones we should look to abide by.

There are many standards out there, and they each have their own way of looking at security. Let's take a look at a few of them:

- **ISO 27001**: Most widely known and accepted information security standard. ISO 27001:2013 consists of 114 security controls across 14 domains of security. It doesn't specifically address cloud security, so it cannot be used as a single source for cloud security.
- **ISO/IEC 27002:2013**: Provides guidelines for security standards but isn't certified against like 27001 is; it's more used for reference.
- **ISO/IEC 27017:2015**: Offers guidelines for information security controls for the provisioning and use of cloud services for both CSPs and cloud customers.
- **SOC 1/SOC 2/SOC 3**: The Service Organizational Control (SOC) is a security control certification program.
    - SOC 1: Focuses on service providers and is related to financial statements.

      Type 1: Auditors' findings at a point in time

      Type 2: Operational effectiveness over a period of time (six months to one year)
    - SOC 2: Meant for IT service providers and cloud providers. Addresses the five Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy), providing a detailed technical report. Also uses a Type 1 and Type 2 report scheme like SOC 1.

    - SOC 3: Covers the same content as SOC 2, but the report only identifies success or failure of the audit and doesn't contain sensitive technical information like the SOC 2 report would.
    - SOC reports are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16 (which replaced SAS 70).
- **NIST SP 800-53**: Used to ensure the appropriate security requirements and controls are applied to US federal government information systems. Risk management framework.
- **PCI DSS**: A security standard with which all organizations that accept, transmit, or store card data must comply. There are four merchant levels based on the number of annual transactions which define the level of compliance required and the amount of audits each must conduct. As a processor, you can never store the credit card verification (CCV) number. There are over 200 controls in the standard.

E2. System/subsystem Product Certifications

Why do we need to verify cloud vendor systems are certified against standards?

- Our data resides on the vendor's systems, and we must "trust" the vendor to maintain confidentiality, integrity, and availability (CIA) of our data.
- Cloud vendors that meet standards are more likely to provide us with the CIA we require, which reduces our risk.
- Imagine using a cloud vendor that has no certifications.
    - We know nothing about their capabilities — only what they tell us.
    - No third-party audits have taken place to validate the vendor's claims.
    - Trusting this vendor would be a high-risk decision.

Common Criteria (CC) Assurance Framework (ISO/IEC 15408-1:2009): International standard designed to provide assurances for security claims by vendors

- Primary goal is to ensure customers that products have been thoroughly tested by third parties and meet the specified requirements.

- CC has two key components:
  - Protection profiles: A standard set of security requirements for a specific type of product, such as firewall, IPS, switch, etc.
  - Evaluation Assurance Levels (EALs): Define how thoroughly the product is tested.

    Sliding scale from 1-7

    1 is the lowest level evaluation, and 7 is the highest.
- CC process:
  - Step 1: Vendor completes a Security Target (ST), which provides an overview of the product's security details.
  - Step 2: A certified lab will test the product to see if it meets specifications in the protection profile.
  - Step 3: A successful evaluation leads to an official certification of the product.

FIPS 140-2: A NIST document that lists accredited and outmoded crypto systems

- The benchmark for validating the effectiveness of cryptographic hardware/systems
- All crypto systems used should meet FIPS 140-2 compliance
- Ensure your cloud vendor is FIPS 140-2 validated
- FIPS is measured by levels 1-4
  - Level 1 is the lowest level of compliance.
  - Level 4 is the highest level of compliance and signifies the product provides the highest level of security.

Domain 2: Cloud Data Security

A. Describe Cloud Data Concepts

A1. Cloud Data Life Cycle Phases

There are *six* phases of the Cloud Data Lifecycle:

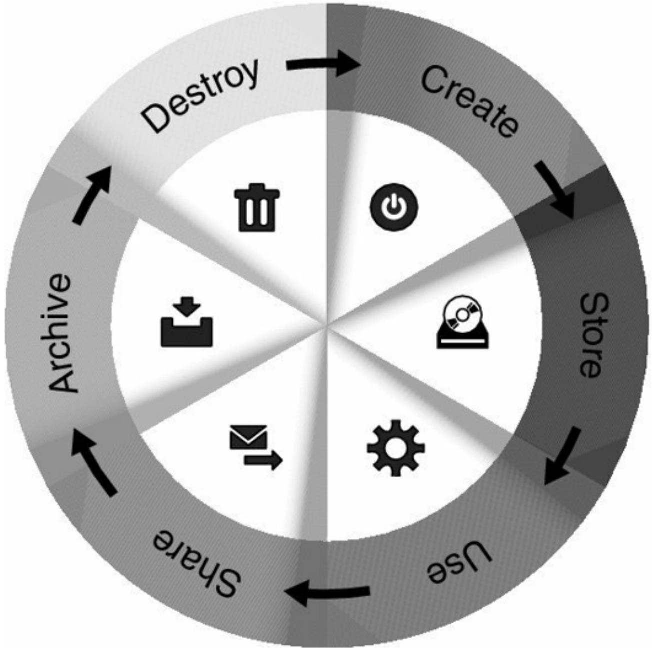
1. **Create**: Data creation, acquisition or altering. Preferred time to classify data.
2. **Store**: Committing data to storage. At this point, implement security controls to protect data (encryption, access policies, monitoring, logging, and backups).
3. **Use**: Data being viewed or processed, not altered. Data is most vulnerable at this point. Controls such as data loss prevention (DLP), information rights management (IRM), and access monitoring should be implemented to protect data at this phase.
4. **Share**: Difficult to manage data once it leaves the organization. DLP and IRM can be helpful to manage what data can be shared.
5. **Archive**: Data no longer actively used is moved to long-term storage. Archived data must still be protected and meet regulatory requirements.
6. **Destroy**: Removal of data from a CSP.

There are three key data functions:

1. **Access**: View and access data.
2. **Process**: Use the data to perform a function.
3. **Store**: Store the data in a database or file system.

Now that we know the data functions, we need to think about controlling these functions:

- **Access**: How do we control data access?
  - Access management (access lists)
  - Encrypt data so non-authorized persons cannot read the data
  - Digital rights management (DRM) to prevent unauthorized access to data
- **Process**: How do we control processing of data?
  - Access management
  - Data encryption
- **Storing**: How do we control storing of data?
  - Policies are a start (USB restriction policy using USBGuard)
  - DRM to prevent copying of data
  - Data loss prevention (DLP) solutions



A2. Data Dispersion

- **Location**: Data moves around between locations. Services are designed to replicate data across geographic regions to guarantee availability. Important data should always be stored in multiple locations for redundancy.
- **Storage slicing/data dispersion**: This is a newer technology in which data is broken into chunks and encrypted, and adds extra bits (erasure coding) used for redundancy, similar to the way RAID works on hard drives. Then the blocks are stored across geographic regions. This allows for retrieval of data in the event multiple data locations go offline.
- **Automation**: Allowing for data to be dispersed automatically. This is why policies surrounding data dispersion is critical. (Ex.: Intellectual property [IP] data cannot leave the continental US.) Also, consider the cost of accidentally replicating terabytes of data across multiple geographical regions. This is another reason dispersion policies are important.
- **IaaS**: Providers offer different classes of service that automatically replicate data across geographically disperse locations.
- **PaaS/SaaS**: Investigate prospective vendors to ensure they practice data dispersion. This may be an additional feature, with additional costs, that is not enabled by default.

B. Design and Implement Cloud Data Storage Architectures

B1. Storage Types

IaaS Storage

- **Volume**: A virtual disk attached to a virtual machine (e.g., VMFS, AWS EBS)
- **Object**: A storage pool like a file share (e.g., AWS S3)

- **Ephemeral**: Temporary storage used while a system is up and running. Once the system shuts down, this storage goes away with all data on it.

PaaS Storage

- **Structured**: Organized data, such as relational databases using tables, keys, rows (e.g., SQL)
- **Unstructured**: Data files such as text files, media files, or other files. Considered unstructured because it's not in a traditional database format (e.g., AWS NoSQL).

Other Storage Types

- **Raw storage**: Raw device mapping (RDM) is an option within VMware virtualization that allows for direct mapping to physical storage such as LUNs
- **Long term**: Data archival services such as Amazon Glacier
- **Content Delivery Network (CDN)**: Content (files) are stored in geographically dispersed object storage, used to improve user experience by increasing delivery speeds

B2. Threats to Storage Types

Threats to Storage Types

- **Unauthorized usage and access**
  - *Cause*: Account hijacking or lack of access control
  - *Resolution*: Multi-factor authentication (MFA) and secure access controls

- **Liability due to regulatory noncompliance**
  - *Cause*: Lack of internal auditing
  - *Resolution*: Implement regulator requirements and self-audit
- **Denial of Service attack (DoS/DDoS)**
  - *Cause*: Lack of edge security
  - *Resolution*: Implement security product to prevent DoS/DDoS
- **Corruption, modification, and destruction**
  - *Cause*: Human or mechanical error
  - *Resolution*: Ensure backups are functional and regularly tested
- **Data leakage and breaches**
  - *Cause*: Holes in security (weak patching, access controls, etc.)
  - *Resolution*: Data loss prevention (DLP) products, penetration tests
- **Theft or loss of media**
  - *Cause*: Unencrypted data being lost or stolen
  - *Resolution*: Encrypt the data at rest (laptops, mobile devices, USB devices, etc.)
- **Malware attack or introduction**
  - *Cause*: Most likely human error
  - *Resolution*: Security training, endpoint protection software (antivirus, antimalware, etc.), network segmentation
- **Improper treatment or sanitization after end of use**
  - *Cause*: Data not being deleted properly
  - *Resolution*: Best option is crypto shredding

    DoD 5220.22-M and NIST 800-88 both deal with data sanitization.

In a cloud environment, unless you have raw data storage (direct disk access), you cannot truly perform the wipe actions as this requires disk access.

Most CSPs put the burden of sanitization on the customer.

Crypto shredding is the best option if you don't have raw disk access.

C. Design and Apply Data Security Technologies and Strategies

C1. Encryption and Key Management

Encryption can be implemented at different points:

- **Data in motion (DIM)**: IPSec can be used via VPN; SSL and TLS can be used across the web.
- **Data at rest (DAR)**: Disk encryption or encryption managed by a storage system.
- **Data in use (DIU):** Information rights management (IRM) and digital rights management (DRM). DRM has been used for the entertainment industry (e.g., CDs, DVDs, software, etc.); IRM is meant more specifically for documents.

Encryption Architecture

- **Data**: The data we want to protect
- **Encryption engine**: Performs the encryption of the data
- **Encryption keys**: Values used during the encryption process later used to decrypt the data

Challenges for Encryption in the Cloud

- Key management is paramount. Whether the key resides with the CSP or the customer, both must protect the key from unauthorized access.
- If the CSP must process encrypted data, there may be issues with indexing of metadata.
- Multitenancy due to shared resources such as RAM where encryption keys could reside temporarily.
- Most often must use software-based encryption, which is more vulnerable to attacks than hardware-based encryption.
- Encryption can impact performance.
- Some solutions force all users and services to go through an encryption engine. This may be a single point of failure and can cause performance issues.
- Data integrity can still be affected with file replacement or tampering. Digital signatures may need to be used to protect file integrity.

Data Encryption in IaaS

- **Basic storage-level encryption**: Only protects from hardware theft or loss. CSPs may still have access to view the data. (Ex.: AWS S3)
- **Volume storage encryption**: Encrypts a storage volume that is mounted and used by the customer through the operation system. Protects against hardware theft or loss, snooping CSP admins, and storage-level backups that could be taken anywhere and viewed. Does not protect against access through the operating system, such as an attacker gaining access.
  - Two methods to implement volume storage encryption:

    Instance-based: The encryption engine resides on the instance itself.

Proxy-based: Encryption engine runs on a proxy instance. This proxy handles encryption and key management and storage. The proxy maps the volume data to the instance for secure access.

- **Object storage encryption**: Since using basic storage-level encryption is known to be less effective, it's best to use external mechanisms to encrypt the data before sending it to the cloud.
  - File-level encryption: Using an IRM or DRM solution will allow for individual file protection.
  - Application-level encryption: The encryption engine resides in the application itself. The application pulls encrypted data, decrypts and processes it, and then re-encrypts it before putting it back on the file system.
- **Database encryption**:
  - File-level encryption: As previously discussed.
  - Transparent encryption: The encryption engine resides within the database itself. Database files are stored encrypted and unencrypted by the database at time of use.
  - Application-level encryption: As previously discussed.

Key Management

- The *most* challenging component of encryption.
- Common challenges when dealing with encryption keys:
  - Access to keys: Regulatory requirements and ensuring CSPs don't have access
  - Key storage: Must be securely stored to prevent access and must be auditable for access
  - Backup and replication: Backup and replication can create the need for long-term key storage

Key Management Considerations

- Keys should always remain in a trusted environment and never transmitted in plaintext
- Loss of keys equals loss of data
- Key management functions should not be done by the CSP to enforce separation of duties

Key Storage in the Cloud

- **Internally managed**: Keys are stored on the virtual machine or application where the encryption engine also resides; protects against lost media.
- **Externally managed**: Keys are stored separate from the encryption engine and data. Must consider how key management is integrated with the encryption engine.
- **Managed by a third party**: Key escrow services

Key Management in Software Environments

- CSPs normally use software-based encryption to avoid costs associated with hardware-level encryption.
- Software-based encryption doesn't meet NIST's FIPS 140-2 or 140-3 specifications. Software encryption has a hard time identifying tampering. May cause an issue if you work with US federal government agencies.

C2. Hashing

Hashing: Using a one-way cryptographic function to create a new value that will replace sensitive data.

Hashing:

- Provides a way to hide sensitive data
- Allows for an integrity check of the data by checking it against the hashed value
- The hashed value in no way can be used to identify the original data

C3. Masking and Obfuscation

- Data obfuscation is the process of changing data so it doesn't appear to be what it is.
- Generally used to comply with standards by masking sensitive data (SSN, DOB, etc.).
- Sometimes used to turn production data into testing data by masking sensitive data points.

Common Approaches to Data Masking

- **Random substitution**: Substitutes sensitive data with random data
- **Algorithmic substitution**: Substitutes sensitive data with algorithmically generated data
- **Shuffle**: Shuffles data around between fields
- **Masking**: Using XXXX to covers up data
- **Deletion**: Deletes the data or uses a null value

Primary Methods of Masking Data

- **Static**: A new sanitized copy of the data is made before use
- **Dynamic**: Data is sanitized while on the move between storage and use

C4. Tokenization

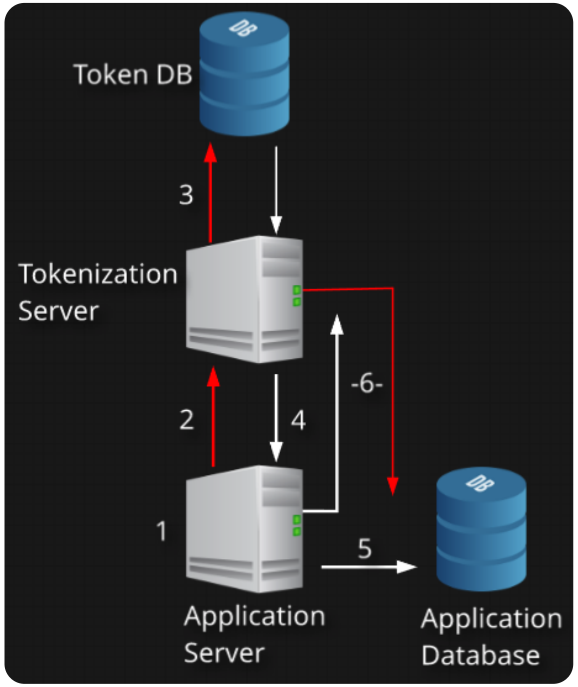
Tokenization: Replacing sensitive data with a non-sensitive piece of data known as a token. This token can map back to the original sensitive information when it needs to be used.

Tokenization can assist with:

- Complying with regulatory requirements
- Reducing the cost of compliance
- Reducing the risk associated with storing sensitive data
- Reducing the attack vectors of sensitive data

Tokenization involves six steps:

1. Sensitive data generation.
2. Data is sent to the tokenization platform.
3. The token is generated, and the sensitive data and token are stored in a database.
4. Tokenization server sends token back to application that generated the sensitive data.
5. The application stores the token.
6. When the sensitive data is needed, the data can be requested by submitting the token.



C5. Data Loss Prevention (DLP)

Data Loss Prevention (DLP): Security controls put in place to prevent certain types of data from leaving the organizational boundaries

- DLP products are available.
- Generally watches for keywords (SSN, DOB, account numbers, etc.) and will prevent that data from leaving the organization via email, file uploads, etc.
- Also known as egress filtering.

DLP Components

- Discovery and classification
- Monitoring
- Enforcement

DLP Architecture

- **Data in motion (DIM)**: Network-based or gateway DLP. Monitors SMTP, HTTP, HTTPS, SSH, FTP, etc., for sensitive data and prevents it from leaving the organization.
- **Data at rest (DAR)**: Storage-based. Used for tracking and identification data as it's installed on the system where the data resides. Generally needs another mechanism for any enforcement.
- **Data in use (DIU)**: Client- or endpoint-based. Resides on users' workstations. Requires great amount of management. Not easy to deploy and manage.

Cloud-Based DLP Considerations

- **Data movement (replication)**: Can be challenging for DLP systems to deal with
- **Administrative access**: Discovery and classification can be difficult in dispersed cloud environments
- **Performance impact**: Network or Gateway DLP solutions can impact network performance, while workstation DLP solutions can slow down endpoints
- **CSP approval**: May need CSP approval to deploy a DLP solution. If it's a hardware solution, this would be hard to get approval for. If it's CSP product, no approval is necessary. If it's software you're deploying into PaaS, then approval is not likely necessary. If deploying a virtual image DLP into IaaS, it's best to check with the CSP.

DLP Policy Considerations

- What classification of data is permitted to be stored in the cloud?
- Where can this data be stored (geographical locations)?
- How should this data be stored (encrypted)?
- What type of access controls need put in place?

- Who, what, where, when, can data be accessed by or from?
- When can data leave the cloud, if ever?

Most cloud vendors offer some sort of DLP service.

C7. Data De-identification

Anonymization: The process of removing direct and indirect identifiers. Can be done by sampling like data and generalizing the data by ensuring the group shares the same value when it comes to sensitive data. This would make it hard to identify a single individual because all the sensitive data is the same between all user data.

Example scenario: In a system, there is a list of addresses. If all the addresses are grouped by zip code, it would make it difficult to pick out the single person who lives in Baltimore if all of the addresses include Baltimore zip codes.

k-anonymity: An industry term used to describe a technique for hiding an individual's identity in a group of similar persons.

Identifier Types

- **Direct**: Data that directly identifies someone (name, address, DOB, SSN, etc.) and is usually classified as PII.
- **Indirect**: Data that indirectly identifies someone (events, dates, demographics, etc.). When combining several of these data points, it may be possible to identify someone.

D. Implement Data Discovery

D1. Structured and Unstructured Data

How do we know what data we have?

- If we don't already know the answer to this question, we need data discovery.
- Maybe we know what data we have, but we want to get more use out of it.

Data discovery can hold more than one meaning

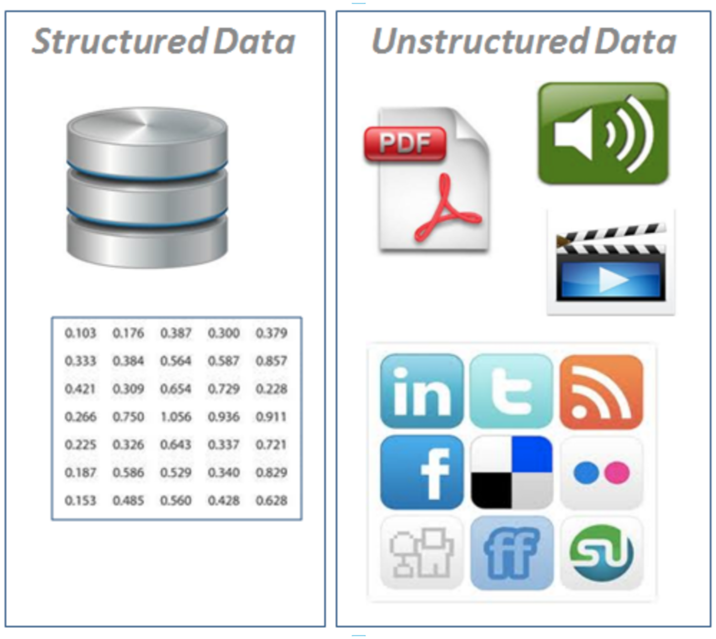
- Working to create a data inventory.
- E-discovery is the process used to collect electronic evidence for a crime.
- Collection and analysis of data in order to find patterns and gain useful insight (data mining, big data, real-time analytics).

Structured data: Data in a structured format, such as a database (SQL)

Unstructured data: Data in an unstructured format, such as a file share (AWS S3, NoSQL)

Data Discovery Approaches

- **Big data**: A way of analyzing very large data sets to extract information
- **Real-time analytics**: Looking for patterns of usage
- **Agile analytics**: Freeform adaptive analysis that focuses on a single problem and doesn't analyze all of the data
- **Business intelligence**: Analyzing data and presenting useful information to help decision makers



0.103	0.176	0.387	0.300	0.379
0.333	0.384	0.564	0.587	0.857
0.421	0.309	0.654	0.729	0.228
0.266	0.750	1.056	0.936	0.911
0.225	0.326	0.643	0.337	0.721
0.187	0.586	0.529	0.340	0.829
0.153	0.485	0.560	0.428	0.628

Data Discovery Techniques

- **Metadata**: Information about the file (owner, size, create date, etc.)
- **Labels**: Labels assigned to data by the owner
- **Content analysis**: Analyzing data content, looking for keywords

Data Discovery Issues

- Poor data quality (no labels, scattered, various formats)
- Hidden costs

Challenges with Data Discovery in the Cloud

- Can be hard to identify where the data is (scattered/replicated)

- Accessing the data

E. Implement Data Classification

Data classification: The process of determining classification categories, and labels. Then identifying the data, recording its location, and labeling the data.

- Requires a good relationship between classifications and labels.
- Organizational policies will determine classifications to be used.
- Data owners will apply labels to adhere to the classifications.

Classifications:

- Confidential, secret, top secret
- Internal only, limited sharing

E1. Mapping

Mapping: Locating data and recording its location, data format, file types, and location type (database, volume, etc.)

E2. Labeling

Labels: Tags applied to data by the data owner which describe the data

Common Labels

- To encrypt, not to encrypt
- Internal use, limited sharing
- Sensitive

- Confidential, secret, top secret

E3. Sensitive data

Sensitive Data

- Intellectual property (IP)
- Patient medical information
- Personally identifiable information (PII) (SSN, passport number, credit report)
- Federally protected data (FERPA) (student information, grades)

Sensitive data is what needs identified, classified, and labeled.

F. Design and Implement Information Rights Management (IRM)

F1. Objectives

Information rights management (IRM): A form of security technology used to protect data by adding independent access controls directly into the data

- Adds an extra layer of access controls on top of the data's inherent controls
- IRM's access controls are embedded into the data object and move with the data
- Can be used to protect data other than documents, such as emails, web pages, databases, etc.
- Often used interchangeably with DRM (digital rights management)

Data rights: Controlling access to data based on centrally managed policies. Who has the right to access the data?

Provisioning

- Each resource must be provisioned with an access policy.
- Each user who accesses data protected by the IRM must be provisioned with an account.

Access Models

- **Mandatory access control (MAC)**: Grants access based on labels such as confidential or secret, according to organizational policy. Most restrictive access model.
- **Role-based access control (RBAC)**: Grants access based on the user's role or responsibility according to organizational policy.
- **Discretionary access control (DAC)**: The system or data owner controls who has access; it's at their discretion.

IRM Challenges in the Cloud

- Each individual resource must be provisioned with an an access policy (heavy management).
- Each user must be provisioned with an account and keys (look into automation of enrollment).
- Most IRM platforms require each user to install a local IRM agent for key management.
- When reading IRM-protected files, the reader software must be IRM aware.
- Mobile platforms have known issues with IRM compatibility.

F2. Appropriate Tools

Capabilities and Tools of IRM Solutions

- These tools are features of an IRM solution
- Persistent protection, whether at rest, in transit, and after distribution
- Content owners can change permissions as needed (view only, no copy, no print) and can expire content even after it's been distributed
- Automatic expiration (data must check in with the IRM solution before being used)
- Continuous audit trail
- Integration with third-party applications, such as email filtering for automated protection of outbound emails
- Disable copy, paste, screen capture, print, and other capabilities

G. Plan and Implement Data Retention, Deletion and Archiving Policies

G1. Data Retention Policies

Data retention policy should contain the following:

- **Retention periods**: How long specific data needs to be kept
    - Will be based on regulatory and legal requirements as well as business risk
    - PCI Requirement 3.1: Organizations should "Keep cardholder data storage to a minimum."
    - HIPAA: Requires some data to be retained for six years
    - IRS: Seven years in some cases
    - What are your organization's data retention requirements?

- **Retention formats**: What type of media is used, if it is encrypted, and the retrieval process
- **Data classification**: How specific data classifications will be stored and retrieved
- **Archiving and retrieval procedures**: Detailed instructions on this process
- **Policy review and enforcement**: How often the policy will be reviewed for effectiveness and who is responsible for enforcing the policy

AWS Config is a service allowing you to assess, audit, and evaluate the configurations of your AWS resources. It provides the ability to create retention policies for data and will auto-delete data based on policy rules.

G2. Data Deletion Procedures and Mechanisms

In the legacy environment:

- Physical destruction of hardware
- Degaussing
- Overwriting with multiple passes
- Crypto shredding: encrypting data, then using a different key to encrypt the data encryption key, then destroying both keys

Cloud data deletion:

- Crypto shredding is the best option

Need to have a data disposal policy that outlines the procedures used to delete or sanitize cloud data.

AWS Data Sanitization Procedures

1. AWS uses techniques outlined in NIST 800-88, "Guidelines for Media Sanitization," when decommissioning customer data.
2. Amazons EFS (Elastic File System) is designed in a way that once data is deleted, it will never be served again.

G3. Data Archiving Procedures and Mechanisms

Data archiving: Process of identifying and moving inactive data from a production system into a long-term archival storage system

Long-term cloud storage is less expensive than production system storage. It is less expensive because it may take several hours to complete the data retrieval process (not instantly available like production data).

Data archiving policies should include:

- Data encryption procedures
  - Long-term key management can be challenging
- Data monitoring procedures to track archived data as it moves around the cloud (must know where data is at all times)
- Ability to retrieve data in a granular manner using e-discovery, which allows for granular searching of the archived data
- Backup and DR options if any archived data is necessary for business continuity (BC)
- Data format should be recorded, as proprietary formats may change over time (MS Office 98 documents may not be able to be opened by a newer MS Office version)
- Data restoration procedures in detail

Data Archival Security Concerns

- Long-term storage of related encryption keys
- Data format (need to maintain software that can read the data)
- Media on which data is stored (will it deteriorate over time?)

G4. Legal Hold

If an organization is involved in litigation (pending legal actions), they may be notified of required compliance with a litigation hold or legal hold.

- At this point, the organization must show good faith efforts in preserving any data related to the case until the obligation no longer applies.
- Routine data retention and destruction procedures must be suspended until the legal hold is over.
- Organization may send out a "litigation hold notice" to internal departments.
- If the organization doesn't comply, they can be guilty of "spoliation," which is a failure to preserve evidence.

AWS Legal Hold Options

- Use a Vault Lock, which allows for a non-readable and non-rewritable format that meets several regulatory requirements dealing with legal holds.
- Legal hold can be enabled on a Glacier Vault (long-term storage) by creating policy that denies the use of delete functions.

H. Design and Implement Auditability, Traceability and Accountability of Data Events

H1. Definition of Event Sources and Requirement of Identity Attribution

Event sources: These are what will be monitored to collect event data

SaaS Event Sources

- Typically have minimal access to event data
- Will most likely only be high-level application-generated log data on client endpoints
- Will need to address this in the cloud SLA or contract specifying what logs you may need access to, such as:
  - Web server logs
  - Application server logs
  - Database logs
  - Network captures
  - Billing records

PaaS Event Sources

- Since the organization is using the PaaS platform to develop on, the organization's development team will need to be worked with to gain an understanding of what logs are available and how to access them.
- According to OWASP, the following application events should be logged:
  - Input validation failures (protocol violations, unacceptable encoding, invalid parameter names and values)

    Could be an attempted injection attack

  - Output validation failures (database record set mismatch, invalid data encoding)
  - Authentication successes and failures
  - Authorization (access control) failures
  - Session management failures (cookie session ID value modification)
  - Application errors and system events (runtime, connectivity, performance, file system errors, third-party errors)
  - Use of high-risk functions (add/remove users, permission changes, privilege changes, assigning of tokens, creation and deletion of tokens, use of sys admin privileges, use of encryption keys, access to sensitive data, creation and deletion of objects, data import and export activities, etc.)

IaaS Event Sources

- Should have access to event and diagnostics data
- Much of the infrastructure logs will be available
- These logs will probably be important at some point:
  - Cloud or network provider perimeter network logs
  - DNS logs
  - VM logs
  - Host OS and hypervisor logs
  - API logs
  - Management portal logs
  - Packet captures
  - Billing records

Event attributes: Information about individual event entries in logs, such as:

- Timestamp
- Event ID
- Application ID (name and version)
- IP address
- Service name
- Geolocation data
- URL, form, web application name
- Code location
- Account involved
- Source address
- Severity
- Description
- Result
- Reason
- HTTP status code
- User type classification (authenticated, authorized)

AWS offers *centralized logging* built upon the Amazon Elasticsearch Service, which allows for collection and analysis of AWS services logs.

H2. Logging, Storage and Analysis of Data Events

Security information and event management (SIEM): A system that collects logs from many systems and provides real-time analysis of the data, providing alerting and reporting for specific events. SIEMs are sold as software, appliances, or as a managed service.

What SIEMs Provide

- **Data aggregation**: Bringing many logs from operating system, network devices, and applications together for analysis
- **Correlation**: Looking for common attributes within the logs that may be used to chain together events
- **Alerting**
- **Dashboards**: Much quicker than reading through reports
- **Compliance**: Can generate compliance reports based on event log data
- **Retention**: Long-term storage
    - Most SIEMs don't provide long-term storage in an active manner. They tend to offload events after a certain age to an internal archival area. This is due to the fact that you could end up with billions upon billions of events over time, and most systems cannot manage that much data efficiently.
- **Forensic analysis**: Searching through logs from many systems by specific date, time, or other criteria

H3. Chain of Custody and Non-repudiation

Chain of custody: The protection and preservation of evidence throughout its life

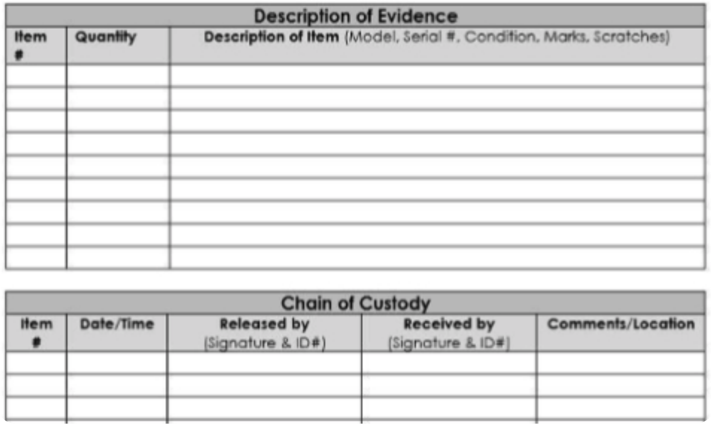
Documentation should exist that shows the following information for evidence:

- When evidence was collected

- Where evidence is located, at what dates, and who placed it there (for storage of evidence)
- Transfer of evidence
- Any access to the evidence
- Any analysis performed on evidence

The chain of custody form should be used for transfer of evidence between individuals.

Chain of custody in the cloud can be very difficult. If your organization is in a regulated industry, you may want to ensure wordage dealing with CSP cooperation with chain of custody practices is included in your contract with the CSP.



Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

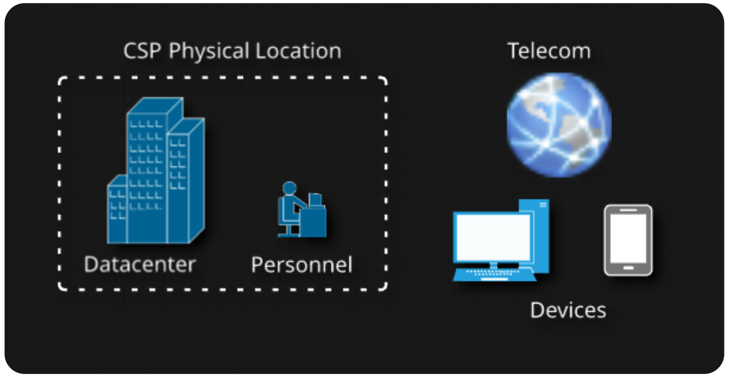
Nonrepudiation: The idea that someone cannot deny something

- Assurance that an individual created a specific item
  - File or email with digital signature of creator
- Assurance that an individual sent an email and another received it (digital signature of sent email, read receipt from receiver)

Domain 3: Cloud Platform and Infrastructure Security

A. Comprehend Cloud Infrastructure Components

A1. Physical Environment



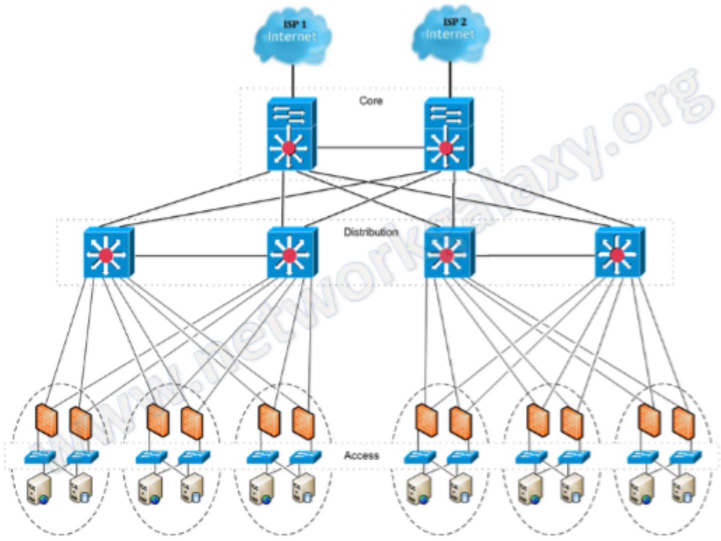
Shared responsibility: The idea that the CSP is not wholly responsible for security, but it is shared responsibility between the customer and the CSP

- In IaaS, the CSP is *not* responsible for:
  - Patching customer virtual machine operating systems
  - Installing and managing security endpoint solutions
  - Managing access lists in the customer's security groups or network rules
  - The customer's virtual environment settings compliance
- In PaaS, the CSP is *not* responsible for:
  - Ensuring customer code is written securely
  - Any compliance the customer's code needs to meet
- In SaaS, the CSP is *not* responsible for:
  - Compliance with how the customer uses the software
  - The type of data entered into the software by the customer's organization

A2. Network and Communications

Remember: Cloud data still runs on hardware!

Cloud carrier: Organization providing connectivity between the CSP and the cloud customer



Network Functionality

- Address allocation (DHCP or static)
- Access control (who can access what)
- Bandwidth allocation (allocation: allocating a percent of bandwidth for a specific use)
- Rate limiting (limiting the amount of traffic)
- Filtering (access lists to close ports, prevent protocols)
- Routing (sending traffic where it needs to go)

Software-defined networking (SDN): Allows for networking to become completely programmable and the underlying hardware is simply commodity hardware. The goal is to make networking more agile, flexible, and centrally managed.

A3. Compute

Compute capacity is dependent on:

- Number of CPUs
- Amount of memory

Reservations: A guaranteed minimum amount of resources to a guest

Limits: Maximum resource allocation

Shares: Each guest is assigned a number of shares and when contention occurs, those shares determine the amount of the available resources that guest receives

A4. Virtualization

Virtualization includes the use of compute, storage, and network.

Capacity monitoring is used to ensure fair, policy-based resource allocation is being provided to tenants of the virtual environment.

Sharing resources enables more efficient use of hardware.

Easier management, which reduces the amount of management labor.

Hypervisor: Software, firmware, or hardware that makes the guest OS think it is running directly on physical hardware

- Allows for multiple guests to run on the same underlying hardware
- Two types of hypervisors:
  - Type 1: Bare metal running directly on hardware (VMware ESXi)
  - Type 2: Runs on top of an OS and provides a virtual environment (VMware Workstation, VirtualBox)

    More susceptible to vulnerabilities
- Risks associated with hypervisors:
  - Vulnerabilities in the hypervisor can lead to guest targeting
  - One tenant may be able to see into another tenant's resources (VM hopping)
  - Resource availability may not function properly, starving a guest OS
  - VM images are files on the hypervisors and susceptible to attacks if securing controls are not put in place

A5. Storage

The primary protection of data at rest is encryption, which helps ensure confidentiality.

Block Storage

Primary role of storage is to group disks together into logical volumes (LUNs, virtual disks, generic volume storage, and elastic block storage)

- None of these have a file system when created
- It's up to the OS on the VM to create the file system

Object Storage Is a Service of CSPs

- Has a flat file system on it
- Provides for simple object storage (files of nearly any type)
- Objects are accessible via browser and REST API
- AWS refers to these as buckets in their S3 service
- Rackspace offers cloud files
- Object storage is typically the best way to store an OS (image)
- Data can be replicated across multiple object storage servers or sites
- Offer basic file usage, nothing fancy

Key Items to Understand about Object Storage

- Takes time for changes to replicate between instances
- Not good for real-time data collaboration
- Best for objects that don't change a lot or are not being collaborated on
- Can be used for backup storage, images, and other static files

A6. Management Plane

Controls the entire infrastructure:

- Allows admins to remotely manage all hosts

Key role of the management plane is to create, provision (create), start/stop VM instances, and live migration of VMs.

Management plane integrates access control, logging, monitoring, and authentication.

Customers have access to part of the management plane via a web management portal, a command line interface, and APIs.

- All of these need to have access controls enabled and verified.

The management plane is very high risk due to the possibility of software vulnerabilities being present, and a vulnerability could lead to access across multiple tenants.

Regulatory requirements may dictate the management network be physically separate.

A management plane's primary interface is its API

- Web GUI is built on top of the API

- API allows for automation
  - Scripting
  - Orchestration
  - Managing user access
  - Configuration management
  - Allocating resources

B. Design a Secure Data Center

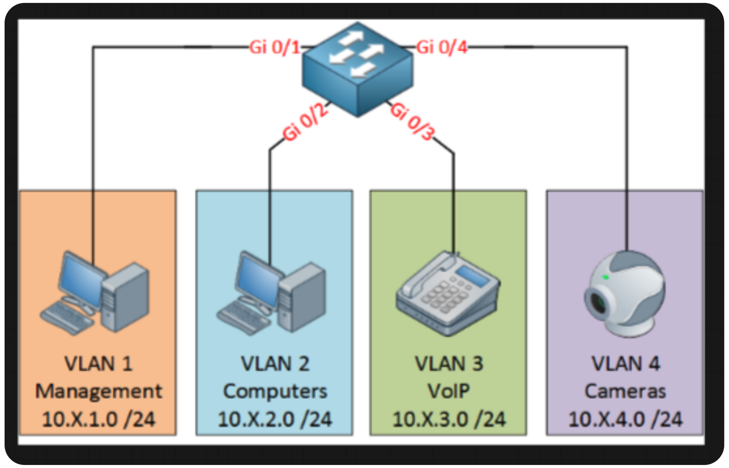
B1. Logical Design

Data center provides many basic services known as "Power, Pipe, and Ping," which relates to:

- Electrical power
- Pipe refers to air conditioning
- Ping refers to network connectivity
- Power and pipe limit the density of servers in a data center

Multitenancy

- Must securely segregate tenants
- Logically separated physical networks (e.g., VLANs)



Cloud Management Plane

- Provide access to monitoring and administration of the cloud environment
- Very high risk (big target)
- Must be logically isolated, but physical isolation would be better

Separation of Duties within CSP Personnel

- Ex.: Backup administrators do not perform audits of backups

Monitoring Capabilities

- Network devices must offer packet-level monitoring
- Hypervisors must provide the ability to monitor activity
- All solutions implemented must provide an acceptable level of audit capabilities

Use of Automation

- Use of secure APIs
- Logging of API activities

Use of software-defined networking (SDN) to support logical isolation

Access Control

- IAM system in use
- IAM system must be auditable

Service Models

- **IaaS**: Hypervisor features can be used to implement security features
- **PaaS**: Logical design features of the platform and database can be used to implement security features
- **SaaS**: Same as PaaS, plus application-level secure features can be implemented

All logical design features should be mapped to a compliance requirement:

- Logging abilities
- Retention periods
- Reporting capabilities

B2. Physical Design

Location

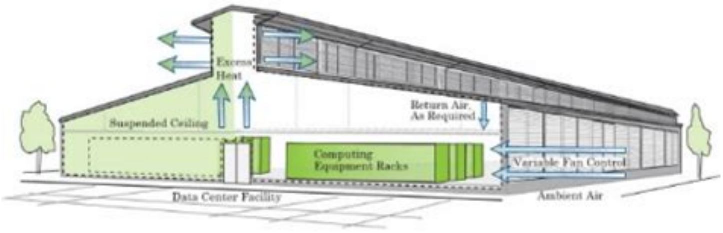
- May impact customer's ability to meet legal and regulatory compliance due to the physical location being in a different jurisdiction
- Must have a clear understanding of all compliance requirements ahead of time

Additional Physical Design Standards

- ISO 27001:2013 - Information technology security techniques
- ITIL - Best practice framework for IT service management (ITSM)

Size of the Data Center

- Use of blade servers for high capacity versus large mainframe servers
- Chicken coop design with cold and hot aisles
- Room for expansion (cooling, power, tenants)



Design Considerations

- Protection against natural disasters
- Access to resources during natural disaster
    - Food

  - Telecommunications
  - Clean water
  - Clean power
  - Accessibility

Protection

- Fences
- Walls
- Gates
- Electronic surveillance
- Ingress and Egress monitoring for audit purposes

Buy or Build

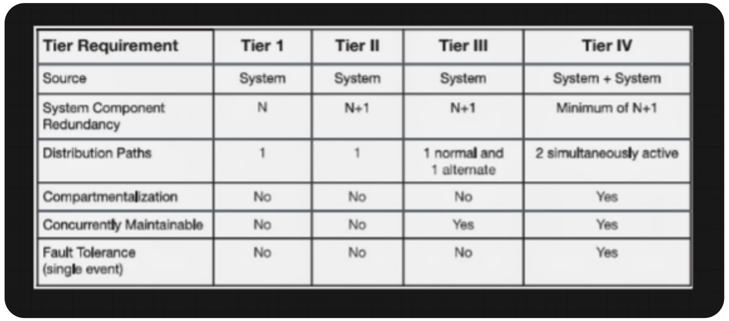
- Data center tier certification
- Physical security
- Usage (dedicated vs. multitenancy)
- Significant investment either way

Data Center Design Standards

- Building Industry Consulting Service International (BICSI): ANSI/BICSI 002-2014 standard covers cabling design and installation.

- International Data Center Authority (IDCA): Infinity Paradigm covers data center location, facility structure, and infrastructure and applications.
- National Fire Protection Association (NFPA): NFPA 75 and 76 specify how hot or cold aisle containment should be done. NFPA standard 70 requires implementation of emergency power-off buttons to protect first responders.

Uptime Institute Data Center Site Infrastructure Tier Standard Topology



Tier Requirement	Tier 1	Tier II	Tier III	Tier IV
Source	System	System	System	System + System
System Component Redundancy	N	N+1	N+1	Minimum of N+1
Distribution Paths	1	1	1 normal and 1 alternate	2 simultaneously active
Compartmentalization	No	No	No	Yes
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerance (single event)	No	No	No	Yes

- Four-tiered architecture, each progressively more secure, reliable, and redundant:
  - Tier 1: Basic data center site infrastructure (basic protection)
  - Tier 2: Redundant site infrastructure capacity components
  - Tier 3: Concurrently maintainable site infrastructure
  - Tier 4: Fault-tolerant site infrastructure (life-dependent applications and services)

B3. Environmental Design

Heating, cooling, ventilation, power, network providers, and paths.

Temperature and Humidity Guidelines

- American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) Technical Committee 9.9 provides guidelines for data center temperature and humidity.
- Temperature: 64.4-80.6°F, 18-27°C (at equipment intake)
- Humidity: 40% @ 41.9°F (5.5'C) to 60% @ 59°F (15°C)

HVAC Considerations

- Lower temperatures equal higher cooling costs.
- Power requirements for cooling are dependent on the amount of heat that must be moved as well as the temperature difference between inside and outside the data center.

Air Management

- Work to prevent any mixing of incoming cool air and exhaust hot air
- Prevents heat-related outages
- Reduces power consumption
- Reduced cooling costs
- Key design issues:
    - Configuring equipment intake and exhaust ports
    - Location of supply and return
    - Large-scale airflow patterns in rooms
    - Set temperature of the airflow

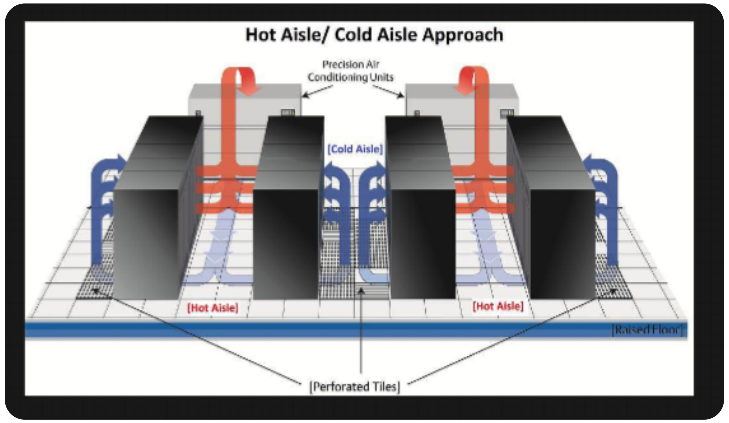
Cable Management

- Minimize airflow obstructions
- Raised floor environments should have 24 inches of clearance
- Cable mining program
    - Ongoing cable management plan to stay on top of it

- A key component to effective air management

Aisle Separation and Containment

- Use of hot and cold aisles
- Designed to prevent the mixing of hot and cold air
- Significantly increases cooling capacity
- Required hardware must be installed in the proper direction
- May have plastic sheeting containing cold aisle
- Holes in rack are covered with blanks



- Raised floors and drop ceilings should be tightly sealed
- Under floor cooling with perforated tiles to the cold aisle is very effective

HVAC Design Considerations

- Local climate will affect HVAC designs
- Redundant HVAC should be used
- HVAC design should include keeping cold and warm air separate
- Energy efficiency should be considered
- Ensure backup power is calculated for HVAC
- HVAC should provide filtering for contaminants and dust

Multi-Vendor Pathway Connectivity

- Redundant connectivity from multiple internet service providers (ISPs)
- Validate ISPs use different back hauls upstream

C. Analyze Risks Associated with Cloud Infrastructure

C1. Risk Assessment and Analysis

Types of Risks

- **Policy and organizational risk**: Related to choosing a CSP and outsourcing
    - Provider lock-in
        - Use favorable contract language (best)
        - Avoid proprietary data formats
    - Provider exit (provider lock-out): Provider is not able or willing to provide services (out of business)
        - Keep data backs on-premises or at another CSP
            - Be careful of interoperability issues with different CSP
    - Loss of governance: Customer being unable to implement all necessary security controls
        - Cloud providers are responsible for defining governance and deploying the related security controls because they own the underlying infrastructure; customers have some input depending on the service model
        - SaaS offers the least amount of control over governance
    - Compliance risks: CSP not being able to provide necessary means for compliance
- **General risk**: Possibility of failure to meet business requirements
    - Consolidation of services can cause a small problem to have a large impact (all eggs in one basket)
    - CSPs built complex environments, which require advanced technical skills
    - Technical risk moves to the provider as they manage the underlying infrastructure
    - Resource exhaustion due to oversubscription or resource failure

- **Legal risks**
  - Data protection: Customer is ultimately responsible for protecting sensitive data such as PII.
  - Jurisdiction: In the cloud, your data may reside in different jurisdictions, affecting regulatory compliance.
  - Law enforcement: If a tenant is mandated to hand over data to law enforcement, it's possible that tenant could inadvertently expose other tenant's data.
  - Licensing: If a customer moves an application to the cloud, the licensing agreement must be reviewed for legality and any cost consequences (per CPU licensing).
  - Data ownership: It's possible a cloud vendor could try to take ownership of data created in the cloud by stating it was created on their platform, therefore they own it. Contractual wording should be used to prevent this.

C2. Cloud Vulnerabilities, Threats and Attacks

Cloud-Specific Risks

- **Management plane breach**: Most important risk because this would give the attacker access to the entire infrastructure.
- **Resource exhaustion**: Oversubscription by the CSP may result in a lack of resources for your cloud services, which may cause an outage
- **Isolation control failure**: When one tenant is able to access another tenant's resources or affect another tenant's resources.
- **Insecure or incomplete data deletion**: Be sure to use crypto shredding.
- **Control conflict risk**: Implementing excessive controls can cause a lack of visibility.
- **Software-related risk**: Software is prone to vulnerabilities and must be kept up to date.
- **Man-in-the-middle attacks**: Cloud solutions increase the risk of man-in-the-middle attacks.

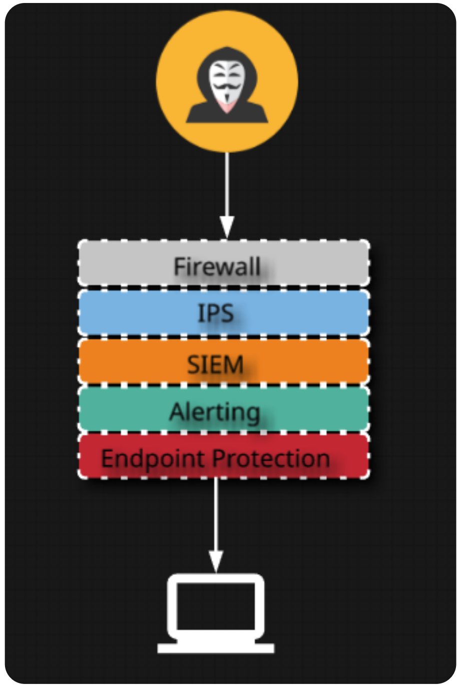
C3. Virtualization Risks

Virtualization Risk

- **Guest breakout/guest escape**: Escape from a guest OS to access the hypervisor.
- **Snapshot and image security**: These may be complete copies of a guest and files are easily moved.
- **Sprawl**: Not managing allocation can allow for over-creation of virtual resources.

C4. Counter-measure Strategies

Multiple layers of defense are needed.



Compensating Controls

- Additional controls that provide backup to primary security controls
- Must have the same intent and level of defense as the original control
- Ex.: Company policy states security measures will be used to control access to sensitive material.
  - Primary control used is standard file system permissions
  - Compensating controls include:

    Use of network access controls (NAC) to prevent unauthorized access onto the network

    SIEM rules to look for and alert on failed attempts to access sensitive data

    DLP system to prevent sensitive data from leaving the organization

    IRM solution to attach additional access controls directly to data in the event it does leave the organization

The Use of Automation

- Using automation for configuration
    - Automates the building of VMs
    - Ensures they'll all be up to standards (updated, patched, security settings, etc.)
    - Reduces human error (forgot to patch something)
    - Allows for updating of a golden or baseline image

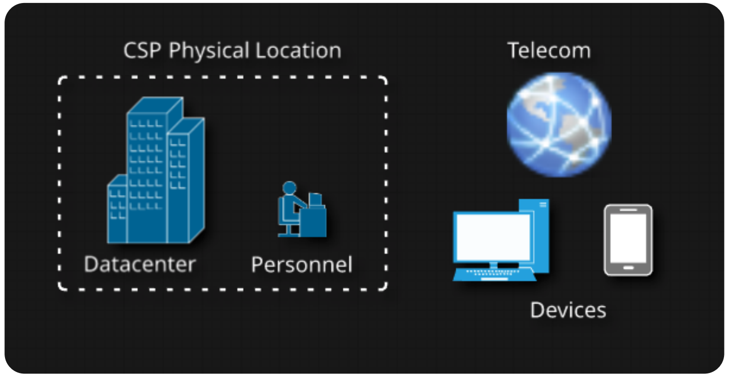
Access Controls

- Physical (doors, locks, biometrics, guards, etc.)
- System (hypervisor, VM OS, network, etc.)
- Role (CSP employee, customer, developer, third-party vendor, remote, auditor, etc.)

D. Design and Plan Security Controls

D1. Physical and Environmental Protection

Physical Security Standards



- NIST SP 800-14 (general principles and practices for securing IT systems)
- NIST SP 800-123 (general servers security)

Key Regulations to CSP Facilities

- PCI DSS
- HIPAA
- NERC CIP (critical infrastructure protection)

Security Control Examples

- Policies and procedures dictate how we implement and manage security controls
- Physical access
- Physical perimeter security (fences, walls, barriers, gates, electronic surveillance, guards)

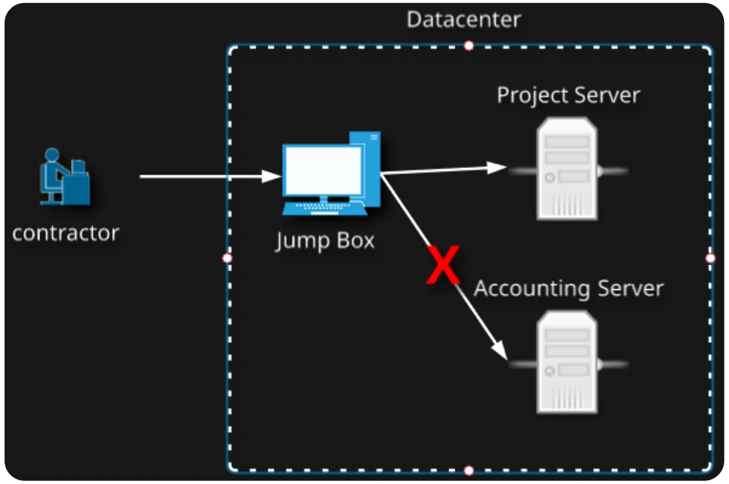
Data Center Protection (to Mitigate Risk

- Multiple layers
  - Guard at gate
  - Badge at gate
  - Badge at main door
  - Guard at main door
  - Biometric check plug badge at each zone with mantrap
- Redundant services (power, cooling, HVAC, etc, networking, etc.)

CSP Personnel

- Background checks and screening
- Training
- Incident response
- More training

D2. System and Communication Protection



Trust zones can be used to segregate network traffic as they are used to control how data is permitted to flow.

- Demilitarized zone (DMZ)
- Location-based zones (departments, buildings, offices, etc.)
- Application zones (prod, dev, DB)

Trust zones control access in both directions (in/out) and protect data's confidentiality and availability.

Data in motion must be protected:

- VLANs can be used to separate data, which helps provide data confidentiality and integrity. VLANs also help reduce resource contention and are very often mandated by compliance standards.
- Encryption is another way to protect encryption in motion by using:
  - VPNs (IPSec)
  - SSL/TLS (HTTPS)
- Within the network, other security controls are available, such as:
  - Firewalls or security groups (access lists)
  - DLP

Data backups:

- To the same CSP as a production environment
  - Speeds up recovery time

- To a secondary CSP
    - Avoids provider lock-out

D3. Virtualization Systems Protection

Snapshotting of images should be considered for use with incident response and any forensic work that needs to be done.

Security controls in virtualization include:

- Traffic control or isolation by using security groups (access lists)
- Guest operating system security software (antivirus, antimalware, etc.)
- Encryption (file and volume)
- Image lifecycle (image creation, distribution, deletion)

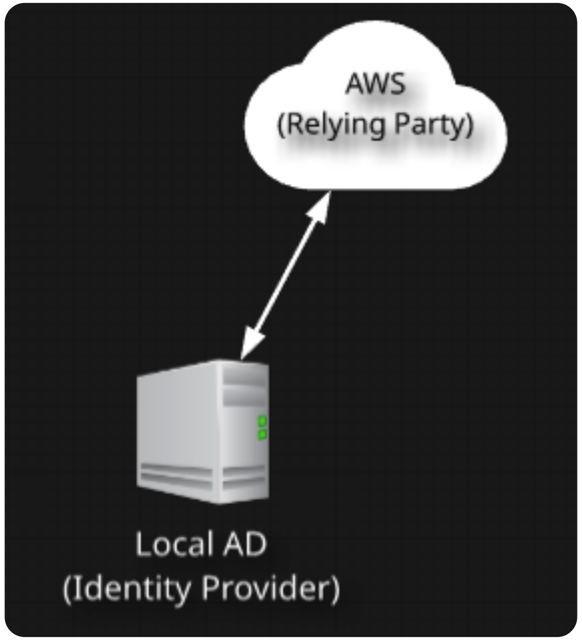
D4. Identification, Authentication and Authorization in Cloud Infrastructure

Identity federation: Trust relationship between multiple identity management platforms at different organizations to provide identity services

- Using local Active Directory authentication to log in to AWS, for example

Identity federation involves two parties:

- **Identity provider**: Responsible for providing authentication
- **Relying party**: Relies on the identity provider for authentication services



Identity Providers

- Use standard authentication protocols, such as OpenID and OAuth
- Many corporate environments use Microsoft Active Directory
- Other protocols are Security Assertion Markup Language (SAML - XML-based) and WS-Federation

Authentication vs. Authorization

- Authentication is the process of validating an identity (identity providers)
- Authorization is the process of granting access to resources (relying party)

Identity Management (Authentication/Identity Provider

- Process of registering, provisioning, and deprovisioning identities

Access Management (Authorization/Relying Party

- Managing an identity's access rights to resources

D5. Audit Mechanisms

Purpose of a risk audit is to provide assurance that proper risk controls are in place and functional.

Reasons for audits:

- Regulatory or legal requirements
- Quality control
- Best practice for security program

Cloud Security Alliance Cloud Controls Matrix (CCM) provides a framework for CSPs to demonstrate adequate risk management.

Audit mechanisms used to collect and provide assurance of proper controls:

- Logs (high-risk events being logged)
- Packet captures (prove HTTP auth denied, only HTTP accepted)
- Config files
- Policies
- Reports (SIEM)

Compliance audits will need to be conducted by a representative (regulator) from the industry or organization when the compliance requirements are set.

Audits of the cloud don't generally include physical access, so the reports may be less complete than an on-premises audit.

Audits of cloud vendor data centers can sometimes be considered less trustworthy because of the reliance on third parties to verify data.

E. Plan Disaster Recovery (DR) and Business Continuity (BC)

E1. Risks Related to the Cloud Environment

Risks That Threaten the Cloud Environment Itself

- Natural disaster (flooding, power, cooling, physical structure damage)
- Equipment failure
- Lack of support staff
- Failure of CSP to provide service (bankruptcy, lack of resources, etc.)

Risks That Threaten BCDR Practices

- BCDR strategies normally include high availability solutions, which are more complicated to manage and can lead to a lack of technical skills
- Equipment failure
- Geographically diverse locations used in BCDR may have network congestion issues
- Regulatory compliance issues if a DR location is in a separate jurisdiction
- Poor encryption key management

Concerns about a BCDR Scenario

- On-premises to CSP failover:
    - Technical capabilities to make this happen

    - Speed at which failover can occur

Failover between Zones within Same CSP

- Are all of the same CSP services available in the failover zone?
- Have the CSP's capabilities been tested?

Failover from One CSP to Another CSP

- Just like selecting a new CSP, must validate thoroughly
- Speed at which the failover can occur
- Impact on end users (will it look different, how do they connect, etc.)

E2. Business Requirements

Recovery Time Objective (RTO): Acceptable amount of downtime for business-critical applications before they need to be functional again after an event

- Must prioritize applications and services
- If less downtime is wanted:
    - Must deploy DR solutions that allow for faster recovery
    - May need more personnel to make this happen
    - May need a hot site instead of a warm site

Recovery Point Objective (RPO): Acceptable amount of data the organization is willing to lose if restoration is required after an event

- Data replication occurs every four hours, so the most the organization would lose is four hours.
- How to lose less?
    - Replication more often
        Increased bandwidth needed
        Licensing requirements

Recovery Service Level (RSL): A percentage (0–100%) of the amount of resources (compute) needed during a disaster based on the service revived during that period

- All services will be restored during a disaster: 100% RSL
- Only the most critical services will be restored during a disaster: 30% RSL
- Completely dependent on organizational requirements

Cloud providers often offer proprietary BCDR technologies that can keep RTO/RPO to near zero.

E3. Business Continuity/Disaster Recovery Strategy

Location

- Is it far enough away from primary location?
- Is it in a separate jurisdiction?
- Can the remote site handle the cutover?
    - Adequate bandwidth and other resources

Data Replication

- Block-level replication protects against data loss but not database corruption
- Look at other options for data types, such as databases
- Must keep in mind storage and bandwidth limitations

Functionality Replication

- Re-creating the same functions at different locations
- Timing is everything!
  - Passive mode: Replicated resources are in standby mode
  - Active mode: Replicated resources are participating in production
- For databases, may look to use Database as a Service if replicating within the same CSP

Other Considerations

- Using a second CSP to replicate to, which may reduce the risk of using a single CSP
- Personal safety is the most important thing

Monitoring is key to failover timeliness.

E4. Creation, Implementation and Testing of Plan

Failover: Options to Switch to BCDR Systems

- Cluster managers
- Load balancers
- DNS changes
- Ensure these are not single points of failure
- Invoking of a BCDR action depends on the contract with the CSP
  - Could be the client or the cloud provider

Return to Normal

- Failback must be considered and tested.
- If not planned, a failback could become a serious outage.
- Sometimes the BCDR site stays active and becomes the new primary site.
- A premature failback could cause serious problems.

Creating a BCDR Plan

- **Define a scope**
  - Roles (who will do what)
  - Risk assessment
  - Policies (determine what constitutes declaring an emergency)

- Awareness so everyone is in the know
- Training (tabletop exercises)

- **Gathering requirements**
    - Identify business-critical services
    - What data is involved?
    - Any service agreements involved
    - List of risks, including failure of any CSPs
    - Determine RTO/RPO
    - Any legal, statutory, or regulatory compliances involved
- **Analysis of the plan**
    - Translate requirements into a design
    - Scope, requirements, budget, performance objectives
    - ID any assets as risk (unrecoverable, corruption, etc.)
    - Identify mitigating controls to be implemented
    - Look at decoupling systems to make BCDR more successful (e.g., applications and databases)
    - Validate CSPs and vendors can meet requirements
    - Identify resource requirements (storage, bandwidth, etc.)
- **Risk assessment**
    - Evaluate CSP's capability to deliver necessary services

        Elasticity

        Contractual issues (if using a second CSP, can they meet contractual needs?)

        Available bandwidth (from customer, to another CSP, between zones)

        Legal and licensing risks (can't have software running in two places without purchasing second license)

- **Plan design**
  - Establish and validate architected solution
  - Include procedures and workflows
  - Define owner(s)
    - Technical (deployment and maintenance)
    - Declaring emergency
    - Communications to customers
    - Internal communications
    - Decision makers in the event of issues
  - How will BCDR plans be tested?
    - Enterprise-wide testing plans should address every business-related service
    - Should be fully tested annually with semi-annual training (walkthrough) or when significant changes occur within business operations
    - Each line within the business should be fully tested to ensure it will survive
    - Testing of any external dependencies
- **Testing policy**
  - RTO/RPO must be measured to ensure attainability
  - Testing objectives should start simple and expand to encompass the entire plan
    - Test individual services
    - Test internal dependencies
    - Test external dependencies
  - Should include test planning
    - Scenarios

        - Measurable results (RTO/RPO)
    - Should include a test scope
        - Master test schedule that includes all objectives
        - Description of test objectives and methods
        - Roles and responsibilities for all participants
        - Define who participants are
        - Key decision makers
        - Test locations
        - Contact information

It's recommended to use the word "exercise" and not "test" when carrying out BCDR validation.

Greater frequency of testing provides greater confidence in BCDR capabilities.

Tabletop Exercises

- Designed to ensure critical personnel are familiar with BCDR and their roles
- Participants follow a pre-planned response
- Not the preferred testing method
- Consists of:
    - Attendance of key personnel
    - Discussion about each person's responsibilities
    - Walkthrough of each step of the procedure
    - Problems identified during testing
    - Provide each participant with a copy of the BCDR plan

Walkthrough Drill/Simulation Test

- More involved than a tabletop exercise
- Participants choose an event scenario and work through the problem on the fly
- Attended by all participants
- Demonstrates knowledge, teamwork, and decision-making capabilities
- Role playing and acting out steps, identifying issues, solving problems
- Involve crisis management team so they can practice as well

Functional Drill/Parallel Test

- Mobilize personnel to other sites
- Establish communications and perform recovery process according to BCDR
- Determine if critical system can be recovered at remote sites and BCDR procedures are adequate
- Testing response procedures
- Parallel processing of data to ensure backup site functionality

Full-Interruption/Full-scale test

- Most comprehensive test
- Must ensure business operations are not negatively affected
- Full BCDR implementation
- Enterprise-wide participation
- Real notifications go out (stating this is an exercise)

- Generally extended over a longer period of time
- Lessons learned, update plan accordingly
- Be sure a full backup occurs prior to the test

Goal of BCDR testing is to ensure the BCP process is:
- Accurate
- Relevant
- Viable under adverse conditions

Business Impact Analysis (BIA

- Determines the RPO/RTO

Domain 4: Cloud Application Security

A. Advocate Training and Awareness for Application Security

A1. Cloud Development Basics

Cloud development typically uses:

- Integrated development environments (IDEs)
- Application lifecycle management
- Application security testing

In most cloud environments, APIs are used to access application functionality, and they use tokens instead of traditional username and password for authentication.

Two of the most common API formats are:

- **Representational State Transfer (REST)**: Consists of guidelines and best practices for creating scalable web services
- **Simple Object Access Protocol (SOAP)**: Protocol for exchanging structured information as part of a web service

Comparing REST and SOAP

- REST supports many formats such as JSON, XML, and YAML, whereas SOAP only supports XML.
- REST uses HTTP/HTTPS for data transfer; SOAP uses HTTP/HTTPS/FTP/SMTP to transfer data.

- REST has good performance and is scalable; SOAP is slower and scaling is complex.
- REST is widely used; SOAP is used when REST is not possible.

A2. Common Pitfalls

- **On-premises does not always transfer to cloud**
    - On-premises apps were not developed for the could environment
    - Cloud may not support the way an application works on-premises
- **Not all apps are cloud ready**
    - Can be more challenging to implement same level of security in the cloud
- **Lack of training**
    - Cloud services may work differently than on-premises alike services
- **Lack of documentation and guidelines**
    - May be lack of documentation by the CCSP if services are new
    - Follow a software development lifecycle (ISO/IEC 12207)
- **Complexities of integration**
    - CSP manages part of the environment and that can make integration tricky since the developers don't see the whole system
- **Overarching challenges**
    - Keep in mind risks such as:

        Multitenancy

        Third-party administrators (CSP)
    - Keep in mind the environment

        Deployment model (public, private, hybrid)

Service model (IaaS, PaaS, SaaS)

Identifying who is responsible for security controls is imperative. Creating a responsibility matrix can be helpful in identifying who is responsible for which security controls.

A3. Common Cloud Vulnerabilities

The most common cloud vulnerabilities are identified in the OWASP Top 10, which we will cover later in this section.

B. Describe the Secure Software Development Life Cycle (SDLC) Process

B1. Business Requirements

Business requirements are included in the first phase of the SDLC where we attempt to identify business needs of the application (accounting, database, customer relations, etc.).

Refrain from identifying technologies at this point — concentrate on the needs of the business.

B2. Phases and Methodologies

Following a software development lifecycle (SDLC) is critical when developing applications for the cloud. ISO/IEC 12207 is one example of an SDLC.

Common SDLC phases across all SDLC versions:

- **Planning and requirement analysis**
    - All stakeholders are involved
    - Business, security, and standard requirements defined

- **Defining**
    - Document all requirements and get a signoff by the customer
- **Designing**
    - Design of the application, which impacts architecture and hardware
    - Threat modeling and secure design elements should be discussed here
- **Developing**
    - Coding starts, and this phase takes the longest
    - Code review, testing, and static analysis is performed
- **Testing**
    - User acceptance testing (end user approval)
    - Testing any integrations
- **Maintenance**
    - Fixing bugs
    - Patching identified vulnerabilities

Once an application goes into production, it enters the secure operations phase.

- Versioning is used to track changes.
- Testing is performed on each version such as dynamic analysis and vulnerability scanning.

When the application is no longer needed, it's time for a disposal phase.

- Crypto shredding is used to erase application data in the cloud.

SDLC for Application Security

ISO has developed the ISO/IEC 27034-1 "Information Technology - Security Techniques - Application Security," which defines concepts, frameworks, and processes to help integrate security into software development lifecycles.

The ISO/IEC 27034-1 is one of the most widely accepted set of standards and guidelines for secure application development.

Part of this standard outlines the organization normative framework (ONF), which consists of:

- **Business context**: Application security policies, standards, and best practices used by the organization
- **Regulatory context**: Standards, laws, and regulations the organization must abide by
- **Technical context**: Required and available technologies that can be used
- **Specifications**: IT functional requirements and solutions to meet the requirements
- **Roles, responsibilities, and qualifications**: Individuals and their roles
- **Processes**: Processes related to application security
- **Application Security Control (ASC) Library**: Contains a list of controls used to protect the application and its data

Application normative framework (ANF): Used in conjunction with the ONF and is created specifically for an individual application. The ONF to ANF is a many-to-one relationship.

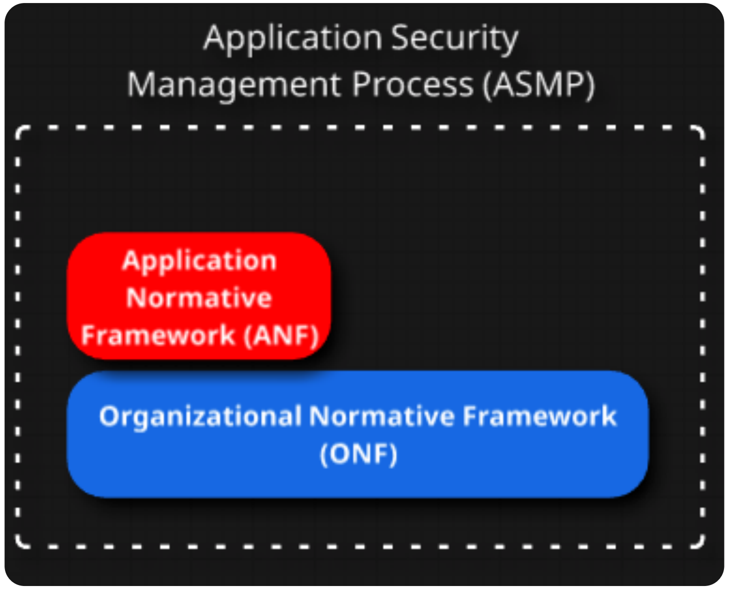
Application security management process (ASMP): Process to manage and maintain each ANF. Consists of five steps:

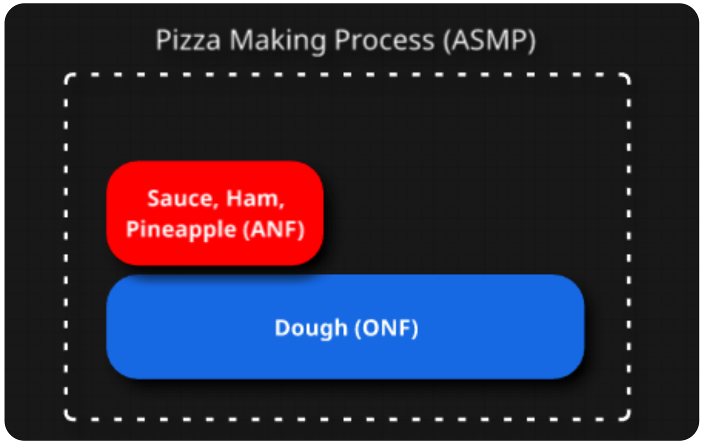
- Specify the application requirements and environment.
- Assess application security risks.
- Create and maintain the ANF.
- Provision and operate the application.
- Audit the security of the application.

C. Apply the Secure Software Development Life Cycle (SDLC)

C1. Avoid Common Vulnerabilities During Development

The most common vulnerabilities are identified in the Open Web Application Security Project (OWASP) Top 10 list. Some of them are listed here (from 2013).


Application Security Management Process (ASMP)
Application Normative Framework (ANF)
Organizational Normative Framework (ONF)



Injection

- SQL injection is a very common example. Injection attacks are when untrusted data in the form of a command or query is sent to an interpreter and executed as a command providing the attacker with information or the ability to execute a command.
  - Prevention: Use input filtering to validate untrusted data meets expected parameters.

Broken Authentication and Session Management

- Improperly implemented authentication mechanisms can allow an attacker to compromise passwords, keys, or session tokens.
  - Prevention: Use proven authentication mechanisms.

Cross-Site Scripting (XSS)

- When a web application accepts untrusted data and sends it to a web browser without proper validation, which can allow an attacker to execute scripts in the victim's browser. Scripts can be posted in a forum, and visitors' browsers will execute the scripts.
  - Prevention: Use "escaping," which is the process of validating code before passing it to an application (making sure it's not malicious).
  - Prevention: Validate inputs to verify the data is not malicious and is expected data.

Insecure Direct Object Reference

- When a developer exposes an internal object, such as a file, directory, or database that can be accessed without authentication.
  - Prevention: Use indirect object referencing where a value is used to represent an object and acts as a go-between so the object itself is never exposed.

Security Misconfiguration

- Mistakes in configuring security settings within an application.
  - Prevention: Know the application and its settings.

Sensitive Data Exposure

- Lack of security controls around sensitive data such as credit card data or PII.
  - Prevention: Use proper security controls, such as encryption, to protect sensitive data.

Missing Function-Level Access Control

- Lack of access control surrounding functions of a web application can allow an attacker to forge requests to gain access to these functions.
    - Prevention: Ensure all functions are accessed via an authorization module, and set a global rule to deny access by default.

Cross-Site Request Forgery (CSRF

- Where an attacker uses an authenticated user's browser to send forged HTTP requests on behalf of the attacker.
    - Prevention: Anti-forgery tokens can be used to prevent CSRF from being successful.

Using Components with Known Vulnerabilities

- Frameworks, libraries, and other software modules can contain vulnerabilities that flow through into any application they're used in.
    - Prevention: Check all components being used for known vulnerabilities, and don't use any vulnerable components.

Invalid Redirects and Forwards

- Web applications sometimes use redirects and forward users to other websites. Without validating these destinations, attackers can cause users to be redirected to malicious websites.
    - Prevention: Avoid using redirects and forwards if possible. If you must use them, avoid involving user parameters in redirecting to the destination.

To identify and address these vulnerabilities, organizations should have an application risk-management program consisting of three parts:

- **Framework core**: Activities and functions divided into five functions:
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
- **Framework profile**: Align activities with business requirements, risk tolerance, and resources.
- **Framework implementation tiers**: Identify where the organization is with its approach.

One popular risk management framework is the NIST Framework for Improving Critical Infrastructure Cybersecurity.

C2. Cloud-specific Risks

Cloud-specific risks include:

- Encryption, because it may need to be built into the application depending on the CSP's architecture.
- Logging may be difficult.
- Ensure applications are using proper access controls.
- PaaS may not offer granular security.

According to the Cloud Security Alliance's "The Notorious Nine: Cloud Computing Top Threats in 2013," the following are the top nine cloud-specific risks:

- Data breaches
- Data loss

- Account hijacking
- Insecure APIs
- Denial of service (DoS)
- Malicious insiders
- Abuse of cloud services
- Insufficient due diligence (on behalf of the customer)
- Shared technology use

C3. Quality Assurance

Validating quality assurance requires measuring variables to ensure quality is being met. These variables include:

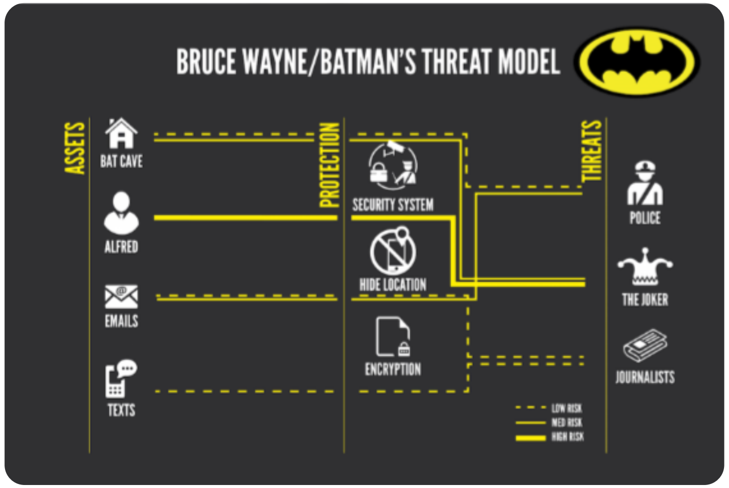
- Availability
- Mean time between failures
- Outage duration
- Performance
- Reliability
- Capacity
- Response time

C4. Threat Modeling

Threat modeling: Works to identify, communicate, and understand threats and mitigations within the context of protecting assets of value.

STRIDE threat model: System for classifying known threats based on the kinds of exploits used or the motivation of the attacker. STRIDE considers the following six threats:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege



C5. Software Configuration Management and Versioning

Proper software configuration management and versioning is an essential part of application security. Two popular tools used for versioning are:

- **Chef**: Used to automate building, deploying, and managing infrastructure components. Configs and policies are stored as recipes. The Chef client is installed on each server, and they poll the Chef server for the latest policy and update their configs automatically based on the Chef server policies.
- **Puppet**: Allows you to define the state of your infrastructure and then enforces the correct state.

The goal of these tools is to ensure configurations are up to date and consistent based on the version of policy or config.

D. Apply Cloud Software Assurance and Validation

D1. Functional Testing

Validates that business requirements have been met and the application operates as expected without errors.

D2. Security Testing Methodologies

Security testing is broken down into two main types:

- **Static Application Security Testing (SAST)**: Considered a white-box test where the test performs an analysis of the source code and binaries without executing the code.
    - SAST is used to identify coding errors that may be an indication of a vulnerability.
    - SAST can be used to find XSS, SQL injection, buffer overflows, and other vulnerabilities.
    - Because it's a white-box test, the results are more comprehensive than dynamic testing.
    - Often run early in the development lifecycle.
- **Dynamic Application Security Testing (DAST)**: Considered a black-box test where the tool must discover vulnerabilities while the application is running. DAST is most effective when testing exposed HTTP and HTML web application interfaces.

SAST and DAST play different roles in application security testing. Where SAST is used early on in development to detect coding problems, DAST is used to identify vulnerabilities of the application while it's running.

Runtime application self-protection (RASP): Prevent attacks by self-protecting or auto-reconfiguring in response to specific conditions.

Vulnerability assessment: Scanning of an application by a vulnerability scanner or assessment tool, such as BURP or OWASP ZAP. These applications look for well-known vulnerabilities and allow for automated scanning. Often run as a white-box test.

Penetration test: Process to collect information about a system and use that to actively exploit any vulnerabilities to gain access to the system or its data. Penetration testing is often considered black-box testing in which the tester has no knowledge of the application.

When performing security testing in a cloud environment, you must receive permission from the CSP in writing prior to performing the testing. Some CSPs provide this on their website while others may require a formal written process.

Secure code review: Manual review of code looking for vulnerabilities.

OWASP has created a testing guide that recommends nine types of testing categories:

- Identity management
- Authentication
- Authorization
- Session management
- Input validation
- Testing for error handling
- Testing for weak cryptography
- Business logic
- Client-side

E. Use Verified Secure Software

E1. Approved Application Programming Interfaces (API)

Application programming interfaces (APIs) are used to expose functionality of an application. APIs provide the following benefits:

- Programmatic control and access

- Automation
- Integration with third-party tools

APIs are components that must be validated for security just as every other component used in the creation and use of applications.

External APIs used by the organization must also go through the same approval process to limit exposure to the organization.

- Use of SSL or other cryptographic means to secure API communications (REST/SOAP)
- Logging of API usage
- Dependency validations using a tool such as OWASP's Dependency-Check

E2. Supply-chain Management

More and more software is being created by third parties and consumed by the masses to build applications and services.

We must keep this in mind and validate all pieces of third-party software being used.

E3. Third Party Software Management

All third-party software should be validated and checked for vulnerabilities before use.

E4. Validated Open Source Software

Open-source software is considered by many to be rather secure simply because the source code is open and available for anyone to view.

- This provides for much scrutinization of the code for best practice and functionality.
- Third-party software is often created in a closed environment with minimal review and testing because time is money.

F. Comprehend the Specifics of Cloud Application Architecture

F1. Supplement Security components

Add additional layers to a defense-in-depth strategy.

Supplemental security components include:

- **Web application firewall (WAF):**
    - Layer 7 firewall that can understand HTTP traffic calls (GET, POST, etc.)
    - Good at preventing DoS attacks
- **Database activity monitoring (DAM):**
    - Layer 7 device that understands SQL commands
    - Can be agent-based on SQL servers or network-based
    - Can detect and stop malicious commands from executing on a SQL server
- **XML Gateway**
    - Act as a go-between for access to an API. The XML gateway can use access rules to prevent access to the APIs.
    - Can implement other controls such as DLP, antivirus, and antimalware services

- **Firewalls**
    - Provide filtering capabilities
- **API Gateway**
    - Filters API traffic before it's processed
    - Can provide access control, rate limiting, logging, metrics, and security filtering

F2. Cryptography

When accessing data in the cloud, you are accessing the data across trusted and untrusted networks, so we need to always protect data. One way to do that is by using encryption.

Protecting Data in Motion

Transport Layer Security (TLS): TLS ensures data privacy and integrity between applications.

Secure Sockets Layer (SSL): The standard technology for creating an encrypted connection between a browser and web server. All data passed is kept private and integral.

Virtual private network (VPN): Encrypts data between two endpoints. These endpoints can be firewalls, VPN concentrator devices, agents installed on a workstation.

Protecting Data at Rest

Whole instance encryption: Used to encrypt everything associated with a virtual machine, such as its volumes, disk IO, and snapshots.

Volume encryption: Used to encrypt a volume on a hard drive. The entire disk is not encrypted, only the volume portion. Full disk encryption should be used to protect the entire hard drive.

File or directory encryption: Used to encrypt individual files or directories.

F3. Sandboxing

A sandbox is an isolated environment in which untrusted data can be tested.

Allows for analysis of applications and data in a secure environment without risk to the production environment.

F4. Application Virtualization and Orchestration

Application virtualization is used to test applications while protecting the underlying OS and other applications on the system. It's a form of sandboxing an individual application on a host. Example solutions are:

- Wine: Allows for some Microsoft applications to run on a Linux platform
- Microsoft App-V
- XenApp

G. Design Appropriate Identity and Access Management (IAM) Solutions

G1. Federated Identity

Federated identity allows for trusted authentication across organizations.

Federation Standards

- **Security Assertion Markup Language (SAML)**: The most common federation standard.
    - SAML is an XML-based framework used for federated communications.

- **WS-Federation**: Defines mechanisms to allow different security realms to federate between each other.
- **OpenID Connect**: Lets developers authenticate their users across websites and apps without having to own and manage password files; doesn't use SOAP, SAML, or XML.
- **OAuth**: Widely used for authorization services in web and mobile applications.
- **Shibboleth**: Heavily used in the education space.

Within a federation, there is an identity provider and a relying party.

Federated identity: Sharing identity information across organizations.

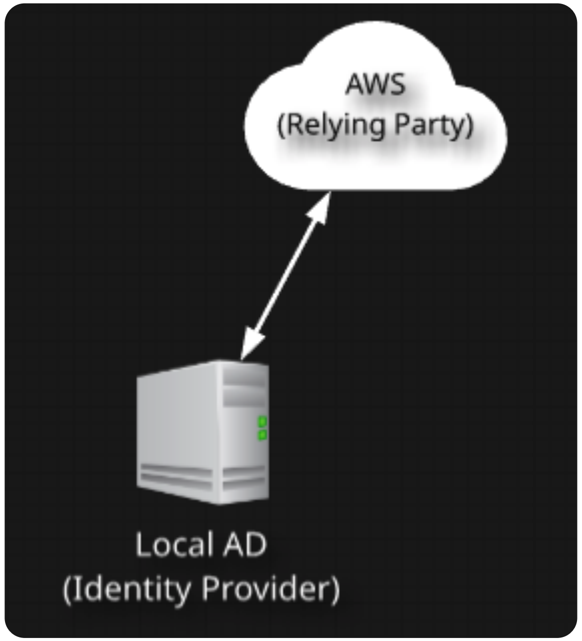
G2. Identity Providers

Identity providers perform authentication services and pass required information on to other parties (relying parties) as needed, which will provide the required authorization to access resources.

G3. Single Sign-On (SSO)

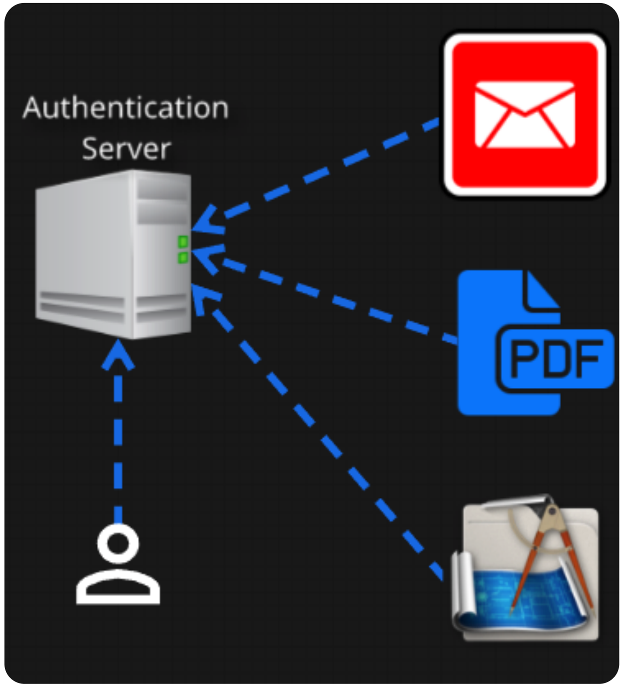
Single sign-on (SSO) allows a user to authenticate once and access several resources, preventing the need to authenticate while accessing each individual resource.

SSO works by having the user log in to an authentication server, and then each resource the user attempts to access checks with the authentication server to verify the user has successfully logged in already.



SSO makes the user experience more pleasant, and all of the SSO happenings are transparent to the end user.

SSO: Sharing identity information across applications.



G4. Multi-factor Authentication (MFA)

Using multiple factors to authenticate. These factors are based on:

- What they know (password, PIN)
- What they have (token, card, Yubikey)
- What they are (biometrics)

One-time passwords fall under MFA and are highly encouraged for use with first-time logins.

Step-up authentication is also used for MFA when accessing a high-risk transaction or violations have occurred in the transaction:

- Challenge questions
- Out-of-band authentication (SMS, text, phone call, etc.)
- Dynamic knowledge-based authentication (question unique to the individual, previous address, etc.)

G5. Cloud Access Security Broker (CASB)

CASB: A trusted third-party identifier that takes on the role of identity provider.

When multiple parties operate in federated identity management (a federation), they must decide to trust each other. This can be done in two ways:

- **Web of trust model**: Each organization has to review and approve each other's members for inclusion in the federation. Can be time-consuming and tedious.
- Outsource to a third-party identifier, such as CASB.

Red Hat Satellite: An infrastructure management product that allows you to manage multiple hosts and environments from a single dashboard. Satellite allows for integration with other Red Hat products such as Insight, which we'll take a look at in just a little bit.

Domain 5. Cloud Security Operations

A. Implement and Build Physical and Logical Infrastructure for Cloud Environment

A1. Hardware Specific Security Configuration Requirements

For Servers

- Follow OS vendor recommendations to securely deploy their OS
- Remove all unnecessary services
- Install all hardware and software vendor patches
- Locking down the host:
    - Restrict root access
    - Only use secure communications for remote access (SSH)
    - Use host-based firewalls
    - Use role-based access controls (RBAC) to restrict user permissions
- Secure management practices
    - Ongoing patching of hardware, OS, and applications
    - Periodic vulnerability scanning of hosts and applications
    - Periodic penetration testing of hosts and applications

A2. Installation and Configuration of Virtualization Management Tools

Extremely important to properly configure virtualization management tools. If compromised, the attacker may have unlimited access to the virtual environment.

All management should occur on an isolated network.

The virtualization vendor will determine what tools are available for use.

- Plan for maintaining these tools and updating them.
- These plans should include a maintenance window or plans for VM migrations between hosts to allow for updates and reboots.
- Vulnerability testing of the tools should be performed.
- Follow vendor guidelines for securely configuring tool sets.

Best Practices

- **Defense in depth**: Use the tools as an additional layer of defense.
- **Access control**: Tightly control and monitor access to these tools.
- **Auditing and monitoring**: Track and validate usage of the tools.
- **Maintenance**: Update tools as necessary and follow vendor recommendations.

A3. Virtual Hardware Specific Security Configuration Requirements

A secure configuration template should be created for each device.

- The template should be saved in a secure manner.

- The template should be updated via a formal change management process.

Virtual hardware should be configured to log sufficient event data.

A4. Installation of Guest Operation System (OS) Virtualization Toolsets

Installation of the virtualization toolsets is one of the most important steps when setting up a cloud environment.

These tools provide additional functionality to virtual machines.

B. Operate Physical and Logical Infrastructure for Cloud Environment

B1. Configure Access Control for Local and Remote Access

Physical access should be limited, and those who manage physical hardware should not have other types of administrative access (separation of duties).

Access to hosts should be done via secure KVM:

- Access to the KVM should be logged and routine audits conducted.
- KVMs provide secure access and prevent data loss.
- MFA should be considered for KVM access.

Secure KVMs meet the following requirements:

- Isolated data channels: Each channel connects to only one host so no data can be transferred between connected computers through the KVM
- Tamper warning labels on each side of the KVM: Indicate tampering
- Housing intrusion detection: Cause the KVM to be inoperable once the housing has been opened

- Fixed firmware: Firmware cannot be reprogrammed; prevents tampering
- Tamper-proof circuit board
- Safe buffer design: No memory buffer to retain data
- Selective USB access: Only recognized human interface USB devices, such as keyboards and mice, to prevent data transfer to USB mass storage devices
- Push-button control: Requires physical access to the KVM to switch between computers

Implement adequate access control measures for KVM access.

B2. Secure Network Configuration

Network Isolation with VLANs

- All environmental management should occur on an isolated network (VLAN).
- VLANs are used to create isolated networks for customers in a multitenancy environment.
- VLANs work by tagging data with a VLAN ID that network devices recognize and are able to use to keep data separate.
- Increase VLAN-related security by:
  - Enabling VLAN pruning (removes unused VLANs)
  - Disabling unnecessary protocols

Transport Layer Security (TLS

- TLS uses x.509 certificates to authenticate a connection and exchange a symmetric encryption key used to securely transmit data between endpoints.

DNSSEC

- Adds security to DNS by enabling DNS responses to be validated.
- DNSSEC uses a process called zone signing that uses digital certificates to sign DNS records.

Threats to DNS

- *Footprinting*: An attacker attempts to gather all DNS records for a domain via domain transfer in order to map out the target environment.
- *Denial of Service (DoS)*: Flooding of DNS servers can prevent the server from responding to DNS requests.
- *Redirection*: An attacker redirects queries to a server under the attacker's control.
- *Spoofing*: Also known as DNS poisoning where the attacker provides incorrect DNS information for a domain to a DNS server, which will then give out that incorrect information.

IPSec

- Protects communications over IP networks with encryption
- Supports peer authentication, data origin authentication, data integrity, encryption, and relay protection mechanisms
- Protects data in transit
- There is a slight performance impact when using IPSec for encryption of data
- Operates in two modes:
    - Tunnel: Encrypts the entire original packet and provides a new header (supports NAT traversal)
    - Transport: Only encrypts part of the original packet

B3. Operating System (OS) Hardening Through the Application of Baselines

Baselines are an agreed-upon set of attributes of a product.

Configuration management tools such as Puppet and Chef can ensure OSes are hardened according to a baseline or policy.

It is important to monitor hosts for baseline compliance and remediate anything out of compliance. To do this, we need to:

- Identify who will perform the remediation (CSP or customer).
- Conduct vulnerability scanning.
- Conduct compliance scanning (OpenSCAP).
- Follow change management processes.

B4. Availability of Stand-alone Hosts

Business requirements may indicate the need for a stand-alone host in a cloud environment.

Downsides of a Stand-Alone Hosts

- Lack of elasticity
- Lack of clustering benefits
- Increased cost

Benefits of a Stand-Alone Host

- Isolation
- Dedicated host
- More secure as it's not on a multitenant host (dedicated server)

Stand-Alone Host Drivers

- Regulatory issues
- Data classification
- Contractual requirements
- Current security policies

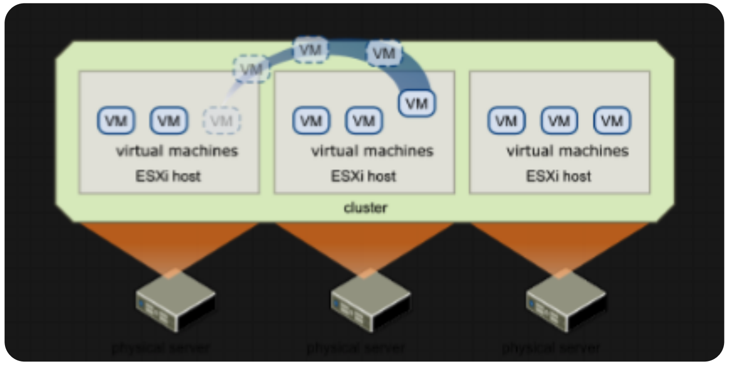
B5. Availability of Clustered Hosts

A host cluster is a group of servers that are centrally managed and allow for failover between hosts and migrating VMs between hosts.

Within a clustered environment, resources are "pooled" and shared. Reservation limits and shares are used to control resource distribution and prevent starvation.

Clusters are used to provide high availability (HA):

- If a host goes down in a cluster, the VMs automatically migrate to another host and power back on.



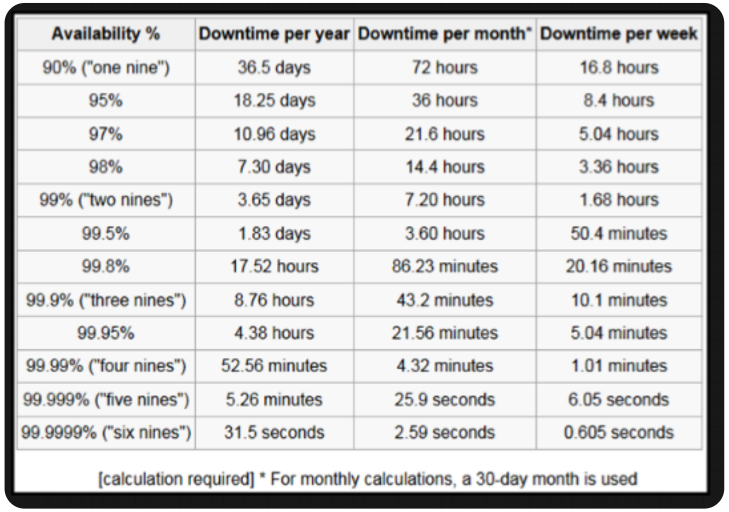
Distributed Resource Scheduling (DRS

- A resource manager that uses rules to balance workloads between hosts
- Affinity and anti-affinity rules can be used to keep VMs together or apart:
  - Redundant DNS servers should not be on the same host.
  - SQL and APP server should be on the same host for best performance.

B6. Availability of Guest Operating Systems (OS)

Availability increases with the use of secure practices, clustering, and high-availability solutions.

Availability is measured in a percentage referred to as nines.



Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

[calculation required] * For monthly calculations, a 30-day month is used

C. Manage Physical and Logical Infrastructure for Cloud Environment

C1. Access Controls for Remote Access

Remote access will need to be provided to employees and third parties.

Key Benefits for a Remote Access Solution

- Accountability of remote access with audit trail
- Session control (access approval, session duration limits, idle timeouts)
- Real-time monitoring of activities and recorded sessions

- Secure access without opening extra ports and increasing the attack surface
- Isolation between the connecting user's desktop and the host being connected to (Virtual Desktop Infrastructure-VDI)

C2. Operating System (OS) Baseline Compliance Monitoring and Remediation

The goal is to ensure real-time monitoring of OS configurations and baseline compliance is happening within the cloud.

Monitoring data should be centrally managed and stored for audit purposes.

Any remediation changes should go through a change management process.

C3. Patch Management

The process of identifying, acquiring, installing and verifying patches for products, applications, and systems.

Patches correct security and functionality problems.

A patch management plan should be developed to manage the installation of patches.

- This plan should be part of the configuration management process.
- Test patches before deployment.

NIST SP 800-40 "Guide to Enterprise Patch Management" is a great reference.

A patch management process should address:

- Vulnerability detection
- Vendor patch notifications
- Patch severity assessment by the organization

- Change management
- Customer notification if required
- Verification of successful patching
- Risk management in case of unexpected outcomes after applying patches (fallback plan)

Patch management challenges:

- Lack of standardization of patches
- Collaboration between multiple system owners
- Many moving parts in large environments
- Patches must be tested before deployment
- VMs in a suspended state (after-hours suspension to save resources)
- Multiple timezones; applying patches at the same local time

In some cases, organizations may give blanket pre-approval for applying patches that address imminent risks, allowing these patches to bypass standard change management process. Change management will happen after the fact.

C4. Performance and Capacity Monitoring

Monitoring of performance and capacity is critical.

- Performance changes can indicate failing hardware.
- Unmonitored capacity could allow for total consumption of resources, which will lead to starvation of resources and serious performance impact.

Items to Monitor on Host Hardware

- Excessive dropped packets on network interfaces
- Disk capacity and IO performance
- Memory utilization
- CPU utilization
- Remember: This is a shared resource environment and to maintain an acceptable level of performance, it must be monitored and managed

C5. Hardware Monitoring

In a virtual environment, everything still runs on underlying hardware and it needs to be monitored:

- Environmental temperature
- Temperature within the hardware (motherboard/CPU)
- Fan speed
- Failed drives or drive errors
- Hardware components (CPU, memory, expansion cards, etc.)
- Network devices as well, not just servers

C6. Configuration of Host and Guest Operating System (OS) Backup and Restore Functions

Host configuration data should be included in any backup plans in the cloud.

Routine tests should be conducted to test restorability of backup data:

- Individual file recovery (file level)
- Entire VMs (image-level recovery)

The biggest challenge with backup and recovery is understanding the extent to which you have access to the hosts and what configurations can be changed.

- **Control**: In the cloud, we make changes through a management interface, but we don't see what happens in the background. We must be confident the changes we make are the only changes occurring.
- **Visibility**: Ability to monitor data and how it's being accessed.

C7. Network Security Controls

Review of Network Security Controls

- Vulnerability assessments
- Network security groups (access lists)
- VLANs
- Access control
- Use of secure protocols, such as TLS and IPSec
- IDP/IPS systems
- Firewalls
- Honeypots
- Zoning of storage traffic (like VLANs for storage data)
- Vendor-specific security products (VMware vCloud Networking and Security or NSX products)

- Keep public data and private data on separate virtual switches

C8. Management Plane

The management plane provides access to manage:

- **Hardware**: Through baseline configurations
- **Logical**: Task scheduling, resource allocation, software updates
- **Networking**: Network management, routes, access lists, security groups, virtual switches, VLANs

Management plane is a high risk and must be protected adequately.

Through the management plane, other actions can occur as well:

- Scheduling of resources through distributed resource scheduling (DRS)
- Orchestration or automation of changes and provisioning
- Maintenance such as software updates and patching

D. Implement Operational Controls and Standards

D1. Change Management

ISO 9001 - Quality and change management: Allows organizations to manage and control the impact of changes to the environment

Change Management Objectives

- Respond to changing business requirements while reducing incidents and disruption.

- Ensure changes are documented in a change management system.
- Ensure changes are prioritized, planned, and tested.
- Optimize overall business risk.

D2. Continuity Management

ISO 22301 - Business continuity: Focuses on planning the necessary procedures for restoring a business to operational state after an event occurs

A prioritized list of systems and services must be created and maintained.

This list is created through a business impact analysis (BIA) which will identify those systems and services critical to the business

Continuity Management Plan

- Defined events to put the plan in motion
- Defined roles and responsibilities
- Defined continuity and recovery procedures
- Required notifications to be made
- Required capability and capacity of backup systems

The business continuity plan should be tested regularly.

D3. Information Security Management

ISO 27001 - Information security management

Organizations should have a documented information security management plan covering:

- Security policies
- Security management
- Asset management
- Physical security
- Access control
- Information systems development, maintenance, and acquisition

D4. Continual Service Improvement Management

ISO 9001 Continuous improvement // ITIL CSI (continuous service improvement): Metrics of all services should be collected and analyzed to look for areas of improvement

The ITIL framework is one resource that can be used to help with this.

D5. Incident Management

ISO 27035 - Security incident management

Purpose of Incident Management

- Restore normal operations as quickly as possible.
- Minimize adverse impact on business operations.
- Ensure service quality and availability are maintained.

D6. Problem Management

ISO 20000 - Problem management: Goal is to minimize impact on the organization by identifying the root cause and implementing a fix or workaround

- **Problem**: The unknown cause of an incident
- **Known error**: A problem with an identified root cause
- **Workaround**: Temporary way of overcoming a problem or known error

A system should be in place to track problems and document root causes and workarounds.

D7. Release and Deployment Management

ISO 20000 - Release and deployment management: Includes planning, scheduling, and controlling the movement of releases to test and live environments

Goal is to ensure the integrity of the live environment is protected.

Objectives of the release and deployment management:

- Define deployment plans.
- Create and test release packages.
- Ensure integrity of release packages.
- Record and track release packages in the Definitive Media Library (DML).
- Manage stakeholders.
- Ensure utility and warranty are met.
    - Utility: Functionality of the product to meet a need
    - Warranty: Product meets agreed-upon requirements
- Manage risks.
- Ensure knowledge transfer.

D8. Configuration Management

ISO 10007 - Quality management (includes configuration management)

A configuration management process should include:

- Development and implementation of new configurations
- Prevention of unauthorized changes to system configurations
- Testing and deployment procedures for system changes
- Quality evaluations of configuration changes

D9. Service level Management

ISO 20000 - Service-level management: Negotiate agreements with parties and design services to meet agreed-upon service-level targets

Typical agreements include:

- **Service-level agreements (SLAs)**: Between customer and provider
- **Operational-level agreements (OLAs)**: SLAs between business units within an organization
- **Underpinning contracts (UCs)**: External contracts between the organization and vendors

Legal department should be included in contract creation, as they can have a financial impact on the provider if SLAs are not met.

D10. Availability Management

ISO 20000 - Availability management process: Define, analyze, plan, measure, and improve availability of IT services

Meet the availability targets set by the organization.

Systems should be designed to meet availability requirements.

The use of high availability (HA) and failover solutions help ensure availability.

D11. Capacity Management

ISO 20000 - Capacity management: Ensures the business IT infrastructure is adequately provisioned to meet SLAs in a cost-effective manner

Capacity must be monitored to ensure an over capacity event doesn't occur that will impact performance and meeting goals.

E. Support Digital Forensics

E1. Forensic Data Collection Methodologies

Forensic Data Collection Process Flow

- Collection of evidence (identify, label, recording, preservation of data integrity)
- Examination (processing of evidence, extracting data while preserving data integrity)
- Analysis (derive useful information from evidence)
- Reporting (reporting on findings, including tools and procedures used, recommendations, and alternate explanations)

The Process

- **Data collection**
  - Develop a plan that prioritizes sources to be collected and in which order they are to be collected:

    Value: Relative likely value of data sources (from past experiences)

    Volatility: Data lost on a system once powered off or after a period of time (page file, memory, logs overwritten by new events, etc.)

    Amount of effort required: Collecting data from an on-premises host versus a cloud vendor's hypervisor. Balance of effort and likelihood data will be valuable.

    Chain of custody should be implemented

- **Acquire the data**
  - Use forensic tools to gather data (write blockers).
  - Create duplicates of data.
  - Secure the original non-volatile data (create a hash if possible).
- **Verify integrity of the data**
  - Use the hashed value of the original data to validate the working copy has not been altered.

Examination

- Extract relevant information from collected evidence.
- May need to bypass OS-level features that may obscure data, such as encryption.
- Use search patterns to look for evidence.
- Tools can help inventory files and categorize them.

Analysis

- Identify people, items, places, data, and events in an effort to piece together a conclusion.
- Use various systems like firewalls, IDS, security management software can help identify events.

Reporting

- There may be more than one possible explanation; be prepared to support all.
- Know your audience: Law enforcement will want details, whereas executives may simply want to know if anything was determined by the evidence.

- Actionable information may be identified that will lead to the need to collect additional information or may be used to identify a way to prevent future events.

Challenges in Collecting Evidence

- Seizure of servers that may contain multiple tenants' data creates a privacy issue.
- Trustworthiness of evidence is based on the CSP.
- Investigations rely on CSP's cooperation.
- CSP technicians collecting data may not follow forensically sound practices.
- Data may be in unknown locations.

Network forensics (capturing of packets) may be necessary to help with a cloud-based investigation.

- Capture of packets can reveal locations (addresses of systems).
- Can provide unencrypted data, such as text files being transferred or emails.
- VoIP streams and video can be captured and replayed as well.

Network Forensics Use Cases

- Identifying proof of an attack
- Troubleshooting performance issues
- Monitoring activity for compliance with policies
- Identifying data leaks
- Creating audit trails

E2. Evidence Management

When collecting evidence, be sure not to collect evidence outside the scope of the event.

Chain of custody is used to manage evidence from identification to disposal.

- **When evidence is collected, the following should be recorded:**
    - Item description
    - Signature of collector
    - Signature of witness
    - Date and time
- **When evidence is stored, the following should be recorded:**
    - Location of storage
    - Signature of person placing the item in storage
    - Signature of person in charge of storage location
    - Date and time
- **When evidence is removed from storage, the following should be recorded:**
    - Item's condition (tampering)
    - Signature of person removing it from storage
    - Signature of person responsible for the storage location
    - Data and time
- **When evidence is transported, the following should be recorded:**
    - Item's point of origin
    - Method of transport
    - Destination

    - Item's condition at point of origin and destination
    - Signature of persons performing the transport
    - Witnesses at departure and arrival locations
    - All points should contain a date and time
- **When any action, process, or testing of evidence occurs, the following should be recorded:**
    - A description of all actions performed along with date and time
    - Signature of person performing the actions
    - Any findings identified during the actions
    - Signature of a witness who was present while actions were performed

Chain of custody is used to prove evidence was secure at all times.

E3. Collect, Acquire and Preserve Digital Evidence

There are many standards covering the collection, acquisition, and preservation of digital evidence:

- ISO/IEC 27037:2012 — Guide for collecting, identifying, and preserving electronic evidence
- ISO/IEC 27042:2015 — Guide for digital evidence analysis
- ISO/IEC 27050-1:2016 — Electronic discovery

F. Manage Communication with Relevant Parties

F1. Vendors and Partners

Identify and document all partners ensuring the relationship is understood:

- Role the partner plays in the business goals

- Any access the partner may have
- Key contacts at the partner organization
- Emergency communication protocols
- Rank the criticality of the partner as it pertains to business needs

There should be a clearly defined on-boarding process for partners, including granting access to systems. Don't forget an off-boarding process as well.

F2. Customers

Organizations have internal and external customers.

- Different clients use services differently, so know your customers
  - Serving internal departments as customers
  - Serving external, paying customers
- Identify individual responsibilities and document them in SLAs

F3. Regulators

Early communication is key when developing a cloud environment.

Regulatory requirements vary greatly based on:

- Geography
- Business type
- Services offered
- Data type

It's imperative a CCSP understand all regulatory compliance needs prior to planning a cloud environment to ensure they can all be met.

G. Manage Security Operations

G1. Security Operations Center (SOC)

A security operations center (SOC) is a command center facility for IT personnel specializing in security. From the SOC IT professionals:

- Monitor the environment for abnormal behaviors and signs of compromise.
- Analyze system logs.
- Protect organizations from attacks.
- Perform vulnerability scans.
- Monitor internet traffic and other traffic flows.
- Asset discovery and management.
- Incident response services.

Most SOCs operate 24/7 and allow for more effective communications between IT security professional working together on a team.

G2. Monitoring of Security Controls

Once security controls are configured and deployed, they must be monitored:

- Firewalls
- IDS/IPS
- Honeypots

- Vulnerability assessments
- Network security groups

All of these security controls create logs that must be captured and analyzed.

G3. Log Capture and Analysis

Various tools are available to collect and analyze log data from (event sources):

- Host servers
- Guest OSes
- Network devices

Centralized and offsite storage of log data can prevent tampering.

Security information and event management (SIEM): Used to centrally collect and analyze logs.

- Can create specific event searches and reporting
- Provides a secondary set of system logs

Logs must be managed or they will overwrite themselves and data may not be available when it's needed.

- Best to offload logs to a centralized log server, such as a SIEM or syslog server
- In the event of a breach, many attackers will wipe system logs to clear their tracks. A SIEM or syslog server will keep a safe copy of the system logs for analysis

G4. Incident Management

Activities of an organization to identify, analyze, and correct hazards to prevent future reoccurrence.

- **Purpose of incident management:**
  - Restore normal operations as quickly as possible.
  - Minimize adverse impact on business operations.
  - Ensure service quality and availability are maintained.
- **Objectives of incident management:**
  - Ensure standardized incident management methods are used.
  - Ensure visibility and communications of incidents to support staff.
  - Align incident management activities with business goals.
- **Incident management plan should contain:**
  - Definitions of an incident
  - CSP and customer roles and responsibilities
  - An incident management process to follow
  - Media coordination
  - Legal or regulatory notification requirements
- **Incident prioritization is made up of:**
  - **Impact**: Effect upon the business
  - **Urgency**: Can resolution be delayed
  - **Priority**: Impact * urgency
- **Incident Response Team (IRT) usually handles these activities.**

Domain 6. Legal, Risk and Compliance

A. Articulate Legal Requirements and Unique Risks within the Cloud Environment

A1. Conflicting International Legislation

Cloud computing introduces many legal challenges for the security professional:

- Conflicting legal requirements
- Lack of clarity

International law: Rules that govern relations between states or countries comprise:

- **International conventions**: Establish rules recognized by conflicting states or territories
- **International customs**: General practice accepted as law
- **General principles**: Laws recognized by civilized nations
- **Judicial decisions**: Determine rules of law

State law: Refers to each US state's local laws within the state court

Copyright and piracy law: Protects the sharing of copyright material with others who are not the legal owners of said material

Enforceable governmental request: An order or request capable of being carried out on behalf of the government (where there is jurisdiction)

Intellectual property (IP) right: Gives the person who created an idea the exclusive right to that idea. Patents, trademarks, and copyrights are legal ways to protect the IP.

Privacy law: Recognition of a person's right to determine what personal information will be released to the public and when that personal information must be destroyed (when it's no longer needed)

The doctrine of the proper law: When a conflicting of laws occurs, this determines the jurisdiction under which the dispute will be heard. Generally based on contractual language through the choice-of-law clause.

Criminal law: A group of rules and statutes to protect the safety and wellbeing of the public

Tort law: These rules and regulations seek out relief for personal suffering as a result of wrongful acts.

- Compensates victims
- Shifts the cost of injuries to the offender
- Discourages careless and risky behavior
- Vindicates interests and rights that have been compromised

Restatement (second) conflict of laws: These are judge-made laws, not legislative-made laws, that come into play when there are regions or states with conflicting laws. The judges must determine which laws are most appropriate for the situation.

A2. Evaluation of Legal Risks Specific to Cloud Computing

One risk is the loss of control of your data in the cloud due to an investigation or legal action being carried out against your organization. To protect yourself, you should:

- Ensure your contract with the CSP states it is to inform you of any such events.

- Ensure the contract states you are to be in control of making decisions about your data and how it's handled in response to a subpoena or similar actions.

A3. Legal Framework and Guidelines

ISO/IEC 27017:2015 - Information technology - security techniques: Covers the use of security controls to protect cloud data and services.

Organization for Economic Cooperation and Development: Privacy and Security Guidelines: The OECD published guidelines governing the privacy and protection of personal data flowing across borders. Focused the need on global privacy protection.

Asia-Pacific Economic Cooperation Privacy Framework (APEC): With 21 member countries, it provides a regional standard to address privacy as an international issue and cross-border data flows. The framework is built upon nine principles:

- Preventing harm
- Notice
- Collection limitation
- Use of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access and correction
- Accountability

EU Data Protection Directive: Provides regulation and protection of personal information within the European Union. Designed to protect all personal data collected about European Union citizens. Its guidelines state:

- Quality of the data: Data must be accurate and kept up to date
- Personal data may only be processed if the person gives consent
- Special categories: It is forbidden to process data related to racial or ethnic origin, political preference, religious beliefs, trade-union affiliation, or data concerning health or sexual status.
- Data subject's right to access data:
    - Confirmation to the data subject if data about that subject is being processed
    - The rectification, erasure, or blocking of data for which the processing does not comply with the provisions of the EU data protection directive

General Data Protection Regulation (GDPR): Goal is to protect all EU citizens from privacy and data breaches. Different from the EU Data Protection Directive in that:

- It applies to all companies processing data of EU citizens no matter the location (globally).
- Organizations in breach of the GDPR can be fined up to 4% of annual global turnover or 20 million pounds — whichever is greater.
- Conditions for consent must not be full of legal jargon but must be in intelligible and easily accessible form.
- Breach notifications must be given within 72 hours.
- Right to be forgotten (data erasure): Entitles the subject to have his/her data erased at will.
- Data portability: The subject has the right to receive a copy of all data from a processor in a machine-readable format and have the right to transmit that data to another processor (controller).
- Denying service because a person doesn't consent to data collection is not permitted.

ePrivacy Directive: Created by the European parliament for the protection of privacy for data for electronic data being processed in the electronic communications sector

Other Legal Requirements to Be Aware Of

- **US federal laws**:
  - *Gramm-Leach-Bliley Act (GLBA)*: Requires financial institutions to explain how they share and protect their customers' data
  - *Health Insurance Portability and Accountability Act (HIPAA)*: Provides data privacy and security provisions for safeguarding medical information

    In order for two HIPAA-compliant organizations to share HIPAA data, they must have a Business Associate Agreement (BAA).
  - *Children's Online Privacy Protection Act (COPPA)*: Created to protect the privacy of children under 13
  - *Federal Trade Commission (FTC)* Requires specific security controls be implemented to protect data
  - *Sarbanes-Oxley Act (SOX)*: Holds company executives accountable for data accuracy in an effort to prevent fraud and protect shareholders and employees
- **US state laws**: Typically a minimum requirement of security controls for contractual obligations
- **Standards**:
  - ISO standards
  - Payment Card Industry (PCI-DSS): Designed to protect cardholder information
- **Silver platter doctrine**: In criminal law, this was a doctrine that a federal court could introduce illegally or improperly state-seized evidence, as long as federal officers had played no role in obtaining it.

> For example: If an employee was stealing sensitive company data and selling it to a competitor and the employer found out, they could collect the proof and hand it over to law enforcement, and that proof could be used legally in court because law enforcement was not involved in collecting the proof.

A4. eDiscovery

E-discovery: Any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case

E-Discovery Challenges

- Identifying everywhere evidence could be located
- Acquiring data from CSPs
- Extracting data from gathered evidence depending on formats
- Cross-border collection of evidence (cooperation from remote CSPs)

Conducting E-Discovery Investigations in the Cloud

- SaaS-based e-discovery: Some packages may be available to help discover, collect, and preserve data in the cloud.
- Hosted e-discovery provider: You can hire a hosted service provider to perform the e-discovery for you.
- Third-party e-discovery: Outsourcing to an organization who specialized in cloud-based e-discovery practices.

A5. Forensic Requirements

Cloud forensics: Practices aimed to reconstruct past cloud computing events by collecting, preserving, analyzing, and interpreting cloud data evidence

Cloud forensics can be difficult because you may not have access to required data and may need to work with a CSP to access the data.

ISO 27050 - eDiscovery: Works to globally standardize the cloud forensic approach

B. Understand Privacy Issues

B1. Difference Between Contractual and Regulated Private Data

Legal responsibility for data processing falls to the customer who signs up for services with a CSP. The customer is ultimately responsible for managing the safety of data it uploads to the CSP.

This includes personally identifiable information (PII) and falls under US privacy law.

PII is data that can be used to identify, contact, or locate a living individual (SSN, driver's license number, address, phone number, date and place of birth, mother's maiden name, or biometric records).

There are two main types of PII related to the cloud:

- **Contractual PII**: Where an organization processes, transmits, or stores PII as part of its business or a service. This data must contractually be protected by the business providing the service.
- **Regulated PII**: When PII must be protected due to legal and statutory requirements based on regulations such as HIPAA and GLBA. Regulatory protection is to protect individuals from risk.
- Both must protect PII, but one is for contractual reasons while the other is for regulatory reasons.
- Another differentiator related to regulated PII is mandatory breach reporting.
- NIST 800-122 is a useful resource for ensuring requirements for contractual and regulated PII are being met.

Contractual Components to Understand as a CCSP

- **Scope of processing**: Identify the types of processing performed with data and what the purpose of the processing is.

- **Use of subcontractors**: Understand where data processing, transmission, and storage of data will take place and any subcontracting involved.
- **Deletion of data**: Verify the data deletion process meets organizational policies.
- **Data security controls**: Security controls should be the same level across the processing organization and any subcontractors.
- **Location of data**: To meet compliance, regulatory, and legal requirements, the location of organizations and subcontractors must be known in order to keep track of the physical location of data.
- **Return of data**: When a contract is terminated, data must be returned in a timely manner.
- **Right to audit**: The customer should have the right to audit the organization performing processing and any subcontractors used in the process.

B2. Country-Specific Legislation Related to Private Data

European Union: The EU has prohibited EU data controllers from transferring personal information data outside their country to non-European Economic Area (EEA) jurisdictions that do not have an adequate level of protection.

- In order for companies to transmit EEA citizens' personal data outside their country, companies must abide by Directive 95/46/EC in the EU, or the Safe Harbor program in the US.

Directive 95/46/EC: Focuses on the protection of individuals as it pertains to processing personal data and the human right to privacy as referenced in the European Convention on Human Rights (ECHR).

EU General Data Protection Regulation (GDPR): Strengthens individual rights to protect their personal data. GDPR introduces some new changes, such as:

- Concept of consent
- Data transfers abroad
- The right to be forgotten
- Establishment of a data protection office role

- Access requests
- Increased sanctions
- Services cannot be denied simply because a person doesn't participate in data collection

The following are ways an entity outside of the EU can be allowed to gather/process privacy data belonging to EU citizens, according to GDPR:

- Be located in a country with a national law complying with EU laws.
- Create binding contractual wording that complies with EU laws.
    - Each country in the EU in which data is processed must approve the contract wording.
- Join the Safe Harbor or Privacy Shield program in its own country.

United States: There is no single federal law governing data protection. There are few restrictions on the transfer of personal data outside the US, which makes it easy to use CSPs located outside the US. However:

- The Federal Trade Commission (FTC) and US regulators hold that the applicable US laws and regulations apply to the data after it leaves the US and the US-regulated entities who send data abroad remain liable for:
    - Data exported outside the US
    - Processing of data by subcontractors outside the US
    - Abroad subcontractors using the same level of protection for regulated data

Safe Harbor program: Developed by the US and EU to address concerns that the US does not have in place a regulatory framework that provides adequate protection for personal data transferred from the European Economic Area (EEA).

- As an alternative to the Safe Harbor program, US organizations can use contractual clauses regulating the transfer of personal data from the EU. Managed by the federal trade commission.

Privacy Shield Framework: As of July 12, 2016, The EU reversed its decision on the legal adequacy of the US Safe Harbor Framework. The US now has the Privacy Shield Framework in place, which the EU deems adequate for protecting personal information. The new Privacy Shield Framework replaces the Safe Harbor program and is managed by the Federal Trade Commission.

Stored Communications Act (SCA): Provides privacy protection for electronic communication and computing services from unauthorized access or interception

Cross-Border Data Transfers: Canadian regulations covering processing of Canadian citizen data outside of Canada

B3. Jurisdictional Differences in Data Privacy

Many other countries such as Switzerland, Argentina, Australia, and New Zealand follow rules similar to the EU's as it pertains to data privacy.

CCSPs should always engage with legal professionals in the area of local and international laws prior to engaging in cloud services.

B4. Standard Privacy Requirements

ISO/IEC 27018: Addresses the privacy aspect of cloud computing and has five key principles:

- **Consent**: CSPs may not use personal data they receive from customers for marketing or advertising without customer consent.
- **Control**: Customers have full control over how CSPs use their data.
- **Transparency**: CSPs must inform customers where their data resides and disclose the use of any subcontractors who will have access to PII.
- **Communications**: CSPs must keep record of any incidents, their response to it, and inform customers.
- **Independent and yearly audit**: To be ISO/IEC 27018 compliant, CSPs must subject themselves to annual third-party audits.

Generally Accepted Privacy Principles (GAPP): The AICPA standard that describes 74 detailed privacy principles, which are very similar to the OECD and GDPR principles

General Data Protection Regulations (GDPR): Data privacy protection for EU citizens covered previously in depth

ISO 27001 Information Security Management System (ISMS): Internal audits should be part of every ISMS, and their goal should be to reduce risks related to the availability, integrity, and confidentiality of data while improving stakeholder confidence in the security posture of the organization.

- ISO 27001 is the most widely used global standard for ISMS implementation.

C. Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

C1. Internal and External Audit Controls

An organization's internal audits act as a third line of defense after security controls and risk management.

Internal audit scopes are directly linked to an organization's risk assessment findings.

External audits focus on the controls over financial reporting.

- Areas that support the financial health of the organization
- Don't necessarily focus on cloud risks

C2. Impact of Audit Requirements

Traditional audit methods may not be applicable in the cloud.

Things to Consider

- How do you know the underlying hypervisor you're auditing is the same one over time?
- How technically understanding is the CSP who's providing you data?
- We can only do our best and attest to what data is provided to us.

C3. Identify Assurance Challenges of Virtualization and Cloud

It's difficult to audit the underlying hypervisors and virtualization of many CCSPs, as they will not provide access to the underlying systems.

Even if an auditor was given access, where would they start? There are thousands of instances, and a customers VMs move around in the CSP's environment.

As a CCSP, we're concerned about verifying confidentiality, integrity, and availability of cloud services. SLAs will generally cover availability but not necessarily confidentiality and integrity.

Auditing in the Cloud for Confidentiality and Integrity

- Understand the virtualization environment, as it will help to plan the assessment and associated testing.
- Validate systems are following best practices when it comes to security.
- Validate configurations are done according to organizational policy.

We must use knowns (best practices, organizational policies, etc.) in our auditing to provide an accurate picture of the cloud environment's compliance.

C4. Types of Audit Reports

Standardized Audit Reports

- **American Institute of CPA's (AICPA's) Service Organizational Control (SOC)1, 2, and 3 reports**
  - SOC 1: Validating financial statements
  - SOC 2: Validating effectiveness of controls in a detailed format

    Type 1: Reporting effectiveness of controls at a point in time

    Type 2: Reporting effectiveness of controls over a period of time (generally six months)
  - SOC 3: Validating effectiveness of controls in a generalized format
- **International Standard on Assurance Engagements (ISAE)**: The international equivalent of a SOC 1 report
- **Agreed-Upon Procedures (AUP)**: Based on the Statement on Standards for Attestation Engagements (SSAE), AUP is where an auditor is engaged to report on findings based on procedures performed by the audited party. The auditor provides no opinion, only states identified facts, and the third party forms their own conclusion on the report.
- **Cloud Security Alliance (CSA)**: Created the Security, Trust, and Assurance Registry (STAR) program
- **EuroCloud Star Audit (ESCA) program**: European CSP certification program

C5. Restrictions of Audit Scope Statements

Audit scope statement: Provides the level of information required for the organization being audited to fully understand the scope, focus, and type of assessment being performed

Audit scope restrictions: Parameters set to focus an auditor's efforts on relevancy and:

- Limit the operational impact of the audit activities
- Lower risk to production environments by audit activities. Examples:
    - Auditor cannot ask for a fully functional disaster recovery test.
    - Auditor cannot pull the fire alarm unannounced to validate functionality.

Cloud service audits are primarily based on:

- Ability to meet SLA (uptime and performance data can be used to validate)
- Contractual requirements
- Industry best practice standards and frameworks such as:
    - The International Standard on Assurance Engagements (ISAE), which is an internal control framework.

Statement on Standards for Attestation Engagements (SSAE): An auditing standard for service organizations that supersedes SAS70

C6. Gap Analysis

Gap analysis: Identifies gaps between an organization's environmental status and frameworks or standards with which that organization is attempting to comply

Ex.: An organization is attempting to comply with PCI-DSS, but they do not have network segmentation for devices handling cardholder information.

The gap analysis helps identify where an organization falls short of compliance so they can remediate those issues to become compliant.

C7. Audit Planning

The Four Phases of Audit Planning

1. **Defining audit objectives**
    - Audit outputs and formats
    - Frequency and focus of audit
    - Number of auditors and subject matter experts (SMEs)
    - Alignment with audit and risk management process
2. **Defining audit scope**
    - Define core focus and boundaries
    - Document services and resources used by CSPs
    - Identify key components of CSP services used
    - Define cloud services to be audited (IaaS, PaaS, SaaS)
    - Define geographic locations to be audited
    - Define the who, what, when, where, why, and how of what will be audited
3. **Conducting the audit (keep the following in mind)**
    - Adequate staff
    - Adequate tools
    - Schedule
    - Supervision of audit
    - Reassessment

4. **Refining the audit process/lessons learned**
   (Review previous audits and take them into account)
    - Ensure scope is still relevant after review
    - Factor in any provider changes since last audit
    - Identify opportunities for report improvements
    - Ensure scope criteria and scope are still accurate after review

C8. Internal Information Security Management System (ISMS)

ISO 27001 Information Security Management System (ISMS): Internal audits should be part of every ISMS, and their goal should be to reduce risks related to the availability, integrity, and confidentiality of data while improving stakeholder confidence in the security posture of the organization.

- ISO 27001 is the most widely used global standard for ISMS implementation

C9. Internal Information Security Controls System

ISO 27001 also covers security control systems within an ISMS.

Security controls are mapped to requirements identified through a formal disk assessment.

ISO 27001 covers several domains including but not limited to:

- A.5: Security Policy Management
- A.8: Organizational Asset Management
- A.10: Cryptography Policy Management
- A.11: Physical Security Management
- A.13: Network Security Management

- A.18: Security Compliance Management

The controls outlined by the ISMS should be used as a minimum acceptable level of security provided by a CSP.

ISMSes assist in standardizing and measuring security across an organization and to the cloud.

C10. Policies

Organizational policies affect the organization as a whole, such as "The organization will follow accepted standards to protect client data."

Functional policies are key to implementing an effective data security strategy.
Examples of functional policies include:

- Data classification policy
- Acceptable use policy
- Data backup policy
- Internet usage policy
- Segregation of duties policy

Cloud computing policies are used to implement effective cloud security. Examples of cloud computing policies are:

- Password policy
- Remote access policy
- Encryption policy
- Third-party access policy
- Segregation of duties policy
- Data backup policy

C11. Identification and Involvement of Relevant Stakeholders

It's extremely important to involve relevant stakeholders from the beginning of a cloud computing discussion. These stakeholders can help provide an overarching view of organizational processes and goals to ensure the approach to cloud fits in and doesn't become a one-off.

- An understanding of current organizational services, operations, and layout must be understood to ensure cloud solutions can meet the needs of each of them.
- Once this data is collected, you may understand the impact on services, people, cost, infrastructure, and stakeholders.

Stakeholder Challenges

- Defining an enterprise architecture. Will need to take into consideration all services across the organization and how they will interoperate.
- Selecting a CSP
- Getting information from persons who may no longer be required after a move to the cloud
- Identifying indirect costs, such as training, new tasks, and new responsibilities.
- Extending risk management to the cloud, as it's a new way of thinking about things

C12. Specialized Compliance Requirements for Highly-Regulated Industries

- **North American Electric Reliability Corporation/Critical Infrastructure Protection (NERC/CIP)**: Specifies the minimum security requirements for operating North America's bulk electrical system
- **Health Insurance Portability and Accountability Act (HIPAA)**: Patient medical information
- **Payment Card Industry (PCI)**: Credit cardholder data
  - Over 200 controls in the standard
  - Four merchant tiers within the PCI-DSS standard based on the number of transactions a merchant processes

- Different merchant tiers dictate the amount of audits each must conduct

C13. Impact of Distributed Information Technology (IT) Model

Clear communications become challenging:

- Remote workers require a re-thinking of internal communication processes.
- Processes must be put in place to address requests in a structured way.
- Multiple geographical locations and timezones may come into play and work schedules may need to be altered.
- Employees in multiple different legal jurisdictions.

Gathering information from resources changes:

- For example, information used to come from a team of employees, and now it comes from members of that group and from a CSP.

Bringing in a third-party consultant to assist with the convergence to a distributed model may be beneficial.

Coordination is key to success in a distributed IT model.

D. Understand Implications of Cloud to Enterprise Risk Management

D1. Assess Providers Risk Management Programs

Assessing a provider's risk management can be done by:

- Reviewing security controls in place
- Identifying methodologies or frameworks used by the provider
- Reviewing provider policies

D2. Difference Between Data Owner/Controller vs. Data Custodian/Processor

Data subject: The person who is the focus of personal data

Data owner: Holds legal rights and complete control of data and can define distribution of said data

Data controller: Person or organization who determines the purposes and the manner in which data is processed

Data custodian: Responsible for the safe custody, transport, storage, and implementation of business rules surrounding data

Data processor: Anyone other than an employee of the data controller who processes the personal data on behalf of the data controller (subcontractor)

- Cloud services are very convenient to consume and can easily cause undue risk due to uncontrolled consumption of services.

Risk profile: An analysis of the types of risks an organization faces

Risk appetite: The level of risk an organization is willing to accept to reach its objectives

D3. Regulatory Transparency Requirements

Many regulations require breach notification to those individuals whose information has been compromised. This includes GDPR (within 72 hours) and HIPAA (no later than 60 days).

Many other regulations require transparency to those individuals whose personal data they maintain, such as GLBA, SOX, and GDPR.

D4. Risk Treatment

There are four general ways to deal with risk:

- **Avoidance**: Simply avoiding risk, such as deciding not to use a specific service because it introduced more than an acceptable amount of risk.
- **Acceptance**: Accept a risk and live with it. Implement security controls around the risk.
- **Transference**: Transfer the risk to another party by outsourcing or insuring against the risk.
- **Mitigation**: Implement a fix to get the risk down to an acceptable level.

Security controls are used to address and control risks. There are three main types of security controls:

- **Physical**: Limiting physical access, such as door locks, fire suppression, fences, guards, etc.
- **Technical**: Logical controls, such as encryption, access lists, firewall rules, etc.
- **Administrative**: Personnel background checks, separation of duties, mandatory vacations, etc.

ISO 27002: Code of practice for information security controls

D5. Different Risk Frameworks

ISO 31000: A guidance standard not intended for certification purposes

- It does not address specific or legal requirements related to risk assessment or management.
- It provides a structured and measurable risk-management approach to assist with identifying cloud-related risks.
- It lists 11 key principles as a guiding set of rules.
- It focuses on risk identification, analysis, and evaluation through risk treatment.

ENISA: Created "Cloud Computing: Benefits, Risks, and Recommendations for Information Security"

- Can be utilized as an effective foundation for risk management.
- It identifies 35 types of risks to consider and the top eight security risks based on likelihood and impact.

NIST - Cloud Computing Synopsis and Recommendations

- Special publication 800-146
- Focuses on risk components and the appropriate analysis of those risks.
- NIST is strongly adopted by the US government and related agencies.

D6. Metrics for Risk Management

Metrics help identify the severity of a risk. Risk programs will use a scorecard to record the severity of specific risks:

- Critical
- High
- Moderate
- Low
- Minimal

Companies often associate a specific dollar amount with each level of risk in order to quantify the amount of risk.

D7. Assessment of Risk Environment

What type of risk does the organization face? This depends on several elements:

- **Service**: What type of cloud services are being used and the risks associated?

- **Vendor**: What is the vendor's reputation? What standards are they compliant with?
- **Infrastructure**: Is the infrastructure following best practices and meeting compliance?

ISO 27002: Code of practice for information security controls

E. Understand Outsourcing and Cloud Contract Design

E1. Business Requirements

Identify the business needs and requirements surrounding the consideration of moving to the cloud.

Define a scope of what will move to the cloud that includes:

- Services included in the move
- Compliances required
- Risks associated with the service and or move

CCSPs should be familiar with the following contract types:

- **Service-level agreement (SLA)**: Sets specific goals for services and their provisions over a timeframe.
- **Master service agreement (MSA)**: A contract entered into by two parties outlining services to be provided. Outlines generic terms, such as payment terms, warranties, intellectual property owners, and dispute resolution.
- **Statement of work (SOW)**: Outlines work to be done as part of a project. Defines deliverables and timelines for a vendor providing service to a client.

E2. Vendor Management

As a CCSP, you must understand that part of dealing with a CSP (vendor) is understanding the associated risks:

- Is this a mature vendor?
- Is the vendor financially stable?
- Is the vendor outsourcing services?
- Is the vendor compliant with industry standards?
- Can the vendor meet my regulatory compliance needs?

In order to understand the risks associated with vendors, it helps to know they are meeting some sort of standard or guideline, such as:

Common Criteria (CC

An international set of guidelines and specifications (ISO/IEC 15408) developed for evaluation information security products to ensure they do what they say they do

CSA STAR

Created to establish transparency and assurance for cloud-based environments. Allows for customers to assess the security of CSPs by asking the CSPs for information who openly provide that information in a transparent manner. CSA STAR is broken into three layers:

- **Self-Assessment**: Requires release of publication of due diligence assessments against the CSA's questionnaire
- **CSA STAR Attestation**: Requires the release and publication of results of a third-party audit of the cloud vendor against CSA CCM and ISO 27001:2013 requirements or an AICPA SOC 2

- **Continuous Auditing**: Requires the release and publication of results related to the security properties of monitoring based on the CloudTrust Protocol

European Union Agency for Cybersecurity (ENISA

- *Cloud Certification Schemes List (CCSL)*
  - Provides an overview of different cloud certification schemes (certifications) and shows the main characteristics of each scheme. It also answers questions such as:

    What are the underlying standards?

    Who issues the certification?

    Is the CSP audited?

    Who performs the audits?
  - CCSL provides information for the following schemes:

    Certified Cloud Service

    CSA Attestation - OCF Level 2

    EuroCloud Star Audit Certification

    ISO/IEC 27001

    PCI-DSS v3

    Service Organization Control (SOC) 1, 2, 3

    Cloud Industry Forum Code of Practice
- *Cloud Certification Schemes Metaframework (CCSM)*: An extension of the CCSL designed to provide a high-level mapping of security requirements of the customer to security objectives in existing cloud security schemes.
  - To access this framework and view different schemes, you can use the "CCSM Online Procurement Tool," which allows you to select your security objectives and will show which security schemes (certifications) include your objectives. **Here is a link** to that tool.

E3. Contract Management

Managing a contract includes:

- Meeting ongoing needs
- Monitoring contract performance
- Adhering to terms
- Managing outages, incidents, violations, or variations

Key contract components:

- Performance measurements (metrics)
- SLAs
- Right to audit
- Definitions
- Termination
- Litigation (issue resolution)
- Assurance
- Compliance
- Access to cloud/data
- Cyber risk insurance
- And much, much more

Failing to address key contract components can result in additional costs to the customer in the event that additions or amendments to the contract are necessary.

E4. Supply-Chain Management

Each supplier added, including CSPs and their subcontractors, increases risk to the organization.

In order to understand ongoing supply chain risks, a CCSP should:

- Obtain regular updates from vendors listing dependencies and reliance on third parties.
- Where single points of failure are identified, vendors should be challenged.
- Continuously monitor suppliers and their changes.

Standards and frameworks to assist with supply chain management:

- NIST SP800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
- ISO 28000: Supply Chain Standard
- ISO 27036: Information Security for Supplier Relationships