Certified Cloud Security Professional (CCSP)

Course Navigation

- **Cloud Concepts, Architecture & Design** — Section 1
- **Cloud Data Security** — Section 2
- **Cloud Platform & Infrastructure Security** — Section 3
- **Cloud Application Security** — Section 4
- **Cloud Security Operations** — Section 5
- **Legal, Risk & Compliance** — Section 6

Exam Preparation

Linux Academy

Cloud Computing Definitions

- **Anything as a Service (XaaS):** A phrase used to describe the many products, tools, and services available via the internet.
- **Apache CloudStack:** An open-source solution for creating, managing, and deploying infrastructure cloud services. A management layer for managing hypervisors.
- **Business Continuity (BC):** The ability of a business to continue to deliver a service or product to its customers following the failure of one or more of its systems.
- **Business Continuity Management (BCM):** A management process that builds a framework based on potential threats and their impact to business operations.
- **Cloud Application Management Platform (CAMP):** A specification designed to help manage applications across cloud platforms.
- **Cloud OS:** A phrase used in place of Platform as a Service (PaaS) as it pertains to cloud computing.
- **Cloud Portability:** The ability to move applications and data between different cloud service providers (CSPs) or between public and private clouds within the same CSP.
- **Desktop as a Service (DaaS):** A virtual desktop infrastructure (VDI) that provides a hosted desktop environment via the internet.

Back
Next

Back to Main

Cloud Computing Definitions (Cont.)

- **Eucalyptus:** An open-source cloud computing and IaaS platform used to manage private and hybrid clouds by interacting with on-premises hypervisors and CSPs.
- **Hybrid Cloud Storage:** A combination of public and private storage. Sensitive data resides on private storage, while non-sensitive data resides in public storage at a CSP.
- **Infrastructure as a Service (IaaS):** A compute infrastructure delivered as a service; includes compute, storage, and networking (a cloud-based virtual environment).
- **Managed Service Provider (MSP):** Provides various IT services such as monitoring, patching, help desk, and network operations center (NOC).
- **Mean Time Between Failures (MTBF):** Measure of the average time between component or system failures.
- **Mean Time to Repair (MTTR):** Measure of the average time it takes to repair a component or system after a failure.
- **Multitenant:** Multiple customers using the same public cloud.
- **Platform as a Service (PaaS):** A cloud-based platform on which clients deploy their applications. The CSP manages the underlying infrastructure; customers only manage their app.

Cloud Computing Definitions (Cont.)

- **Private Cloud:** An internal or corporate cloud that is protected by a corporate firewall and under the control of the local IT department, not the CSP.
- **Recovery Point Objective (RPO):** How much data must be restored from backup after an event. *How much data is the company willing to lose?*
- **Recovery Time Objective (RTO):** How quickly individual services need to be restored after a disaster or critical failure.
- **Scalability:** The ability to increase resources to meet demand.
- **Software as a Service (SaaS):** Cloud-based software offered to clients across the internet, most often as a web-based service. Think web-based applications you log in to and use online.
- **Vertical Cloud Computing:** The optimization of cloud services for a specific industry.

Cloud Computing Roles

- **Cloud Customer:** An individual or organization that uses cloud-based services.
- **Cloud Service Provider (CSP):** A company that provides cloud services to customers.
- **Cloud Service Auditor:** A third party that ensures CSPs are meeting Service Level Agreements (SLAs).
- **Cloud Service Broker (CSB):** An organization that seeks to add value to cloud services through relationships with multiple CSPs. Helps customers identify the best cloud solutions for them and sometimes resells cloud services.
- **Cloud Service Partner:** Any role besides customer that supports or works with a CSP (includes roles such as cloud service auditor and cloud service broker).

Cloud Computing Characteristics

On-Demand Self-Service: Ability of cloud service customers to provision new cloud services or increase existing services on demand.
- Can be dangerous — these services don't require approval by another process, simply the click of a button.

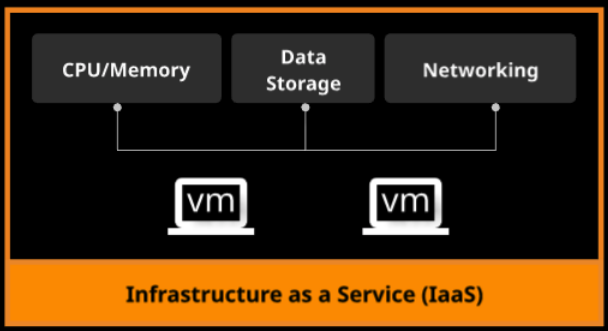
Broad Network Access: The idea that customers should never experience network bottlenecks due to use of technologies such as routing, load balancers, multiple sites, etc.

Resource Pool: CSPs own a large pool of resources (compute, storage, network, etc.), and customers each get an amount of these pooled resources.
- Vast majority of these resources are shared, not dedicated.
- CSPs can spend less money on resources because in a shared environment they are much more efficient.
- CSPs can pass this **savings** on to customers.

Elasticity: Ability to not only scale up, but also scale back resources as needed so you are not paying for unused resources.

Metered or Measured Service: Customer is only charged for what resources they use. Allows for tracking of usage within an organization so individual consumers (departments) can be billed internally.

Building-Block Technologies

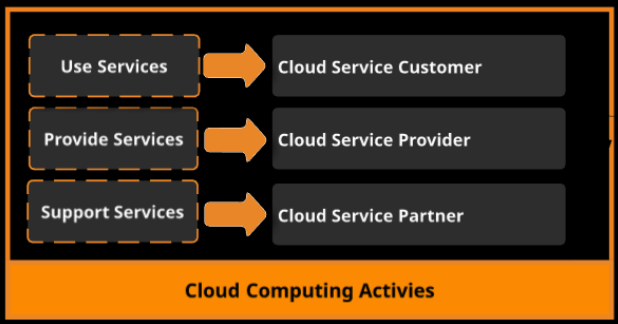


- **CSPs:** Provide CPU, memory, storage, networking, and overall virtualization technology.
- **Customers**: Provide OS, middleware, and applications.

Cloud Computing Activities

Cloud activities fall into 3 groups:

- Activities that **use** services
- Activities that **provide** services
- Activities that **support** services



Activities that use services (cloud service customer)

- Use **cloud services** (create accounts and resources)
- Perform a **trial** (proof of concept)
- Monitor **services** (validate SLAs)
- Administer **security** (manage policies, organize data, audit)
- Provide **billing usage reports**
- **Handle problems** (assess impact, troubleshoot, remedy)
- Select and **purchase** services

Back
Next

Back to Main

Cloud Computing Activities (Cont.)

Activities that provide services (cloud service provider)

- Cloud operations manager (prepare, monitor, manage)
- 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 representatives
- 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)

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, assess marketplace, create legal agreements)

Cloud Computing Capabilities

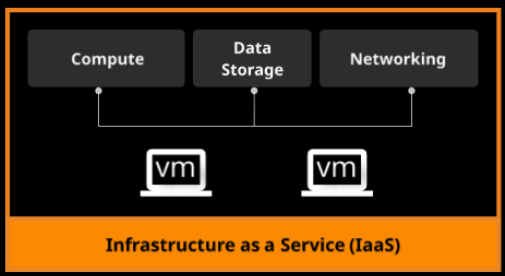
Cloud services can be classified according to **3 capabilities:**

- **Application capability**
  - Where the cloud service customer (CSC) uses the CSP's applications
- **Infrastructure capability**
  - Where the CSC can provision and use the compute, storage, or networking resources of the CSP
- **Platform capability**
  - Where the CSC can deploy, manage, and run their own applications using one or more programming languages and one or more execution environments supported by the CSP

Cloud Service Categories

Infrastructure as a Service (IaaS)

- Cloud service customer can **provision and use** compute, storage, networking, and other services
- **Key components and characteristics**:
  - Scale
  - Combined network and IT capacity pool
  - Self-service and on-demand capacity
  - High reliability and resilience
- **Key benefits**:
  - Measured/metered use
  - Scalability
  - Elasticity
  - Reduced TCO
    - No replacement costs
    - No maintenance fees
    - No cooling or power requirements
    - No up-front hardware or licensing costs (CapEx)

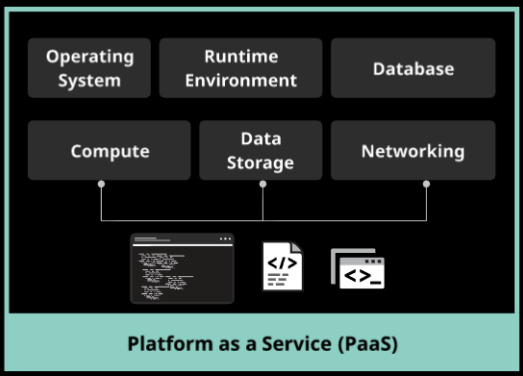


Back
Next
Back to Main

Cloud Service Categories (Cont.)

Platform as a Service (PaaS)

- Customers can **deploy and manage their own applications** using various programming languages and execution platforms.
- **Key capabilities:**
  - Supports multiple languages and frameworks
  - Multiple hosting environments (private, public, etc.)
  - Flexibility
  - Allows for choices of how to create and deploy apps
- **Key benefits:**
  - OS can be changed or upgraded frequently
  - Global collaboration by developers
  - Technology isn't crossing borders; it's cloud-based
  - Cost reduction — single vendor can meet many needs

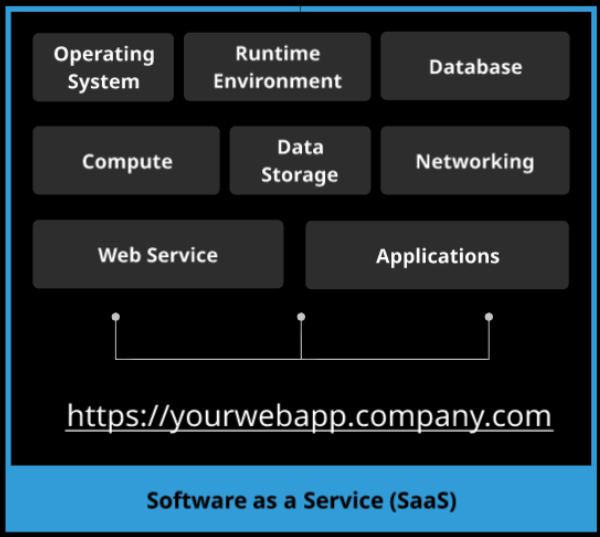


Cloud Service Categories (Cont.)

- **Software as a Service (SaaS)**
  - Customer uses **CSP-provided applications**
  - **SaaS Delivery Models:**
    - Hosted application (HA) management
      - CSP hosts commercially available software across the internet
        - Webmail
        - Accounting apps
        - HR apps
    - Software on demand
      - CSP gives network-based access to a single copy of an application set up specifically for that customer
      - Scales as needed; licenses scale as well
  - **Financial Benefits:**
    - Cost reduction
      - No hardware to purchase or upgrade
      - No support contracts for hardware
    - Licensing
      - No need to purchase licenses up front
      - Licenses are part of the cost
      - Move from CapEx to OpEx
    - Reduces support cost
      - No support contracts to purchase
      - Support handled by the CSP
  - **Other Key Benefits:**
    - Ease of use (less labor to administer environment)
    - Patching and updates are handled by the CSP
    - Standardization (all users on same platform)
    - Global access

Cloud Service Categories (Cont.)

Software as a Service (SaaS)



Communications as a Service (CaaS)

- Provides customers with real-time interaction and collaboration services.

Back

Next

Cloud Service Categories (Cont.)

Compute as a Service (CompaaS)
- Provides customers the ability to provision and use processing resources needed to deploy and run software

Data Storage as a Service (DSaaS)
- Provides customers the ability to provision and use data storage and related capabilities (Ex: Dropbox, Google Docs)

Network as a Service (NaaS)
- Provides customers the ability to use transport connectivity and related network capabilities (Ex: CDNs and VPNs)

Cloud Deployment Models

Four Main Cloud Deployment Models:
- Public
- Private
- Hybrid
- Community

Criteria for Selecting a Cloud Deployment Model:
- Risk appetite
- Cost
- Compliance and regulatory requirements
- Legal obligations
- Business strategy

Public Cloud Model
- A cloud infrastructure **provisioned for use by anyone** who is a customer. Exists on the premises of the CSP.

- **Benefits:**
  - Easy and inexpensive to set up
  - Ease of use
  - Scalable
  - Pay as you go; no wasted resources

- **Examples:**
  - AWS
  - Azure
  - Google Cloud

Cloud Deployment Models (Cont.)

- **Private Cloud Model**
  - A cloud infrastructure **provisioned for use by a single organization**
    - May consist of multiple internal consumers
    - May be owned, managed, and operated by:
      - The single organization
      - A third party
      - A combination of the two
    - May exist on or off the premises of the organization

- **Benefits:**
  - Increased control over everything
  - Ownership and retention of governance controls
  - Assurance of data location
    - Simplified legal and compliance requirements

- **Most often used in large environments with compliance or regulatory requirements**

Cloud Deployment Models (Cont.)

Hybrid Cloud Model

- A combination of two or more cloud models that remain unique entities

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

Community Cloud Model

- Cloud infrastructure provisioned for use by a specific community of consumers that have shared concerns (mission, security requirements, policy, compliance, etc.)

- **Benefits:**
  - Flexibility and scalability
  - High availability and reliability
  - Security and compliance
  - Improved services
  - Reduced (shared) costs

- **Example:** A group of doctors who all use the same medical applications may opt to create a community cloud for a group of practices to ensure compliance and reduce costs.

Cloud Shared Considerations

- **Auditability:** The ability to collect and make available evidential information related to events within a cloud service.
  - What logs are available?
  - What additional charges may be incurred for log access?
- **Availability:** The state of being accessible and usable.
- **Governance:** The system by which the provisioning and use of cloud services is directed and controlled.
- **Interoperability:** The ability of a cloud service customer to interface with the cloud service, or the ability of cloud services to interface with each other.
- **Maintenance:** Maintenance and upgrades can change the way services function; therefore, it's important that the customer be made aware of these activities.
  - Notification of maintenance and scheduled upgrades
  - Disclosure of roll-back practices
  - SLA should document maintenance practices
- **Versioning:** Labeling of a service's version for easy identification. If significant changes are being made, both the old and new versions should be made available in parallel to reduce impact to customers.
- **Performance:** Cloud services should meet metrics defined in the SLA, such as availability, response time, throughput, etc.

Cloud Shared Considerations (Cont.)

Portability: The ability to easily migrate data between cloud service providers and between the cloud and on-premises infrastructure.

Protection of Personally Identifiable Information (PII): CSPs must protect PII, and it should be documented in the SLA. PII is any information that can be used to identify someone, such as a social security number, date of birth, or driver's license number.

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: The ability of CSPs to recover customer data in the event of deletion and the ability of a CSP to delete a customer's data in its entirety (the right to be forgotten).

Security: This includes many capabilities, such as access control, confidentiality, integrity, and availability (the CIA triad). Also includes management and administrative functions.

Service Level Agreement (SLA): Lays out measurable elements needed to assure an agreed-upon quality of service between the cloud service customer and provider.
- The key term is **"measurable"**
- An SLA should include **specific metrics**

Impact of Related Technology

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 **resources** to build environments for this type of data analysis.

Blockchain: A protocol that uses a decentralized framework to maintain integrity within the data.

- Cloud was originally the idea of **off-loading** services to a cloud vendor.
- Blockchain could be used to manage **globally distributed workloads** between data centers so the data resides in multiple data centers at once.
- Not only would this allow for a new type of **decentralized cloud**, but it could also be used to guarantee data integrity.

Internet of Things (IoT): IoT devices are generally sensors or other devices that complete **simple tasks**. Of course the "Internet" in IoT indicates these devices are internet-connected and upload data to an online destination.

- Many cloud vendors offer **IoT services**, including creating images for devices, cloud-based data analysis, and the integration of AI.

Impact of Related Technology (Cont.)

Containers: A container is a small package of code that includes an application, its dependencies, and libraries. That's it! The container then uses the underlying container operating system it runs on for other services such as networking.

- Containers are like a stripped-down version of virtualized **virtual machines** (VMs).
- Containers are **very small** and require very few resources.
- Containers start quickly, as they are tiny.
- Can **scale** very quickly.
- Containers are designed to do a single job, such as host a web service.
- This allows for separating services into individual containers to **increase resiliency and security.**

Quantum Computing: Quantum computing gets its massive compute power by tapping into quantum physics instead of using 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.
- Quantum computing is still in its **infancy.**
- Eventually CSPs will provide **quantum computing services.**

Cryptography and Key Management

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

Data in Transit/Motion

- The movement of data across **untrusted networks**
  - The internet
  - Between cloud providers
- **Secure Socket Layer (SSL)** and **Transport Layer Security (TLS)**
  - SSL uses private and public keys to encrypt data.
  - TLS provides a secure transport "tunnel," often used with mail services.
- **IPSEC**
  - Used in network-to-network VPN tunnel
  - Uses cryptography algorithms such as 3DES and SHA

Data at Rest

- Data **not in use** by users or applications
- Encryption can impact **performance**
- Only required for **sensitive data (PII, PCI, HIPAA, IP, etc.)**
  - Personally Identifiable Information (PII)
  - Payment Card Industry (PCI)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Intellectual Property (IP)
- **Reduces risk** of unauthorized data access
- Can make it hard for the owner to **retrieve the data**
  - Lost encryption keys
  - Dispute with CSP

Cryptography and Key Management (Cont.)

- **Key Management**
  - **Separation of duties** is very 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 Services (KMS)**
      - Customer maintains the KMS on premises.
      - Connectivity is required between KMS server and encrypted cloud data for encryption/decryption.
    - **Client-Side Key Management**
      - CSP provides the KMS, but it resides on customer premises.
      - Customer generates keys, encrypts data, and uploads it to the cloud.

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.**

Identity and Access Management (IAM)
- Controls access to resources by people, processes, and systems
- Validates identity
- Grants level of access to data, services, and applications
- Generally uses a minimum of two factors of authentication to validate user identities.

Key Phases of IAM
- Provisioning and deprovisioning accounts
  - Don't forget to **deprovision old accounts!**
  - **Remove** unnecessary permissions when roles change.
- **Centralized directory services**
  - Store, process, and maintain a centralized repository.
  - Primary protocol is **Lightweight Directory Access Protocol (LDAP)** based on the X.500 standard.

Access Control (Cont.)

- **IAM Key Phases (Cont.)**
  - **Privileged Identity Management (PIM)**
    - An identity management system that includes features such as:
      - **Privileged access** management
      - **Time-based** rules
      - **Geo-based** rules
      - **Audit** capabilities
      - **Notification** capabilities
      - Forced use of **MFA**
    - IAM should use features of PIM for **admin accounts**
      - MFA should ***always*** be used for admin accounts
    - Trust and confidence in the accuracy and integrity of the directory service is **paramount!**
    - Privileged user management
      - Carry the **highest risk and impact**
      - Key component; pertains to privileged accounts
        - Usage **tracking**
        - Authentication success and failure tracking
        - Authorization **dates and times**
        - **Reporting** capabilities
        - Password management (complexity, MFA)
      - Requirements should be **based on organizational policies**
    - Authorization and access management
      - **Authorization** determines a user's right to access a resource.
      - **Access management** is the process of providing access to that resource.

Data and Media Sanitization

Data and Media Sanitization

- The ability to remove all data from a system is critical to **ensuring confidentiality** in the cloud.
- We don't want to leave behind data remnants for someone else to find in the **future.**

How Can We Sanitize Data?

- **Cryptographic Erasure:** Erase, overwrite with a pattern, erase again.
- **Overwriting:** Simply overwriting data may be sufficient for some data but not sensitive data (PII, PCI, HIPAA, IP, etc.)
  - Remember:
    - Simply **deleting** data doesn't actually get rid of it.
    - It only **hides** it from users' view.
    - It's still there until the OS overwrites its blocks with other data.
- **Key destruction** of an encryption key is not sufficient, as the key could be recovered forensically.
- **NOTE:**
  - Without **degaussing** media or physically destroying it, an attacker may be able to recover data.
  - Overwriting data is merely a **deterrent.**

Network Security

Network Perimeter of a CSP
- Can be hard to identify, as it could be anything from a carrier's trunk into a building to a series of micro-instances running as load balancers.

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

Network Security Groups
- **Access lists** permitting or denying traffic
- Can be placed at the **network or VM level**

Virtualization Security

Hypervisor

- Allows multiple operating systems to **share** a single hardware host.
- Types of hypervisors:
  - **Type 1**
    - Bare metal hypervisor that runs **directly on hardware** using a hypervisor operating system.
    - Examples: VMware, ESxi, and Citrix XenServer
    - Related to hardware security.
    - Reduced attack surface because of locked-down OS.
    - Vendor controls the software and all packages.
    - **Increased reliability and robustness,** due to closed environment.
  - **Type 2**
    - Runs on a **host OS** and provides virtualization services.
    - Examples: VMware Workstation and Virtual Box
    - Relates more to OS security (underlying OS).
    - **More attractive to attackers** because of the number of vulnerabilities in underlying OS and installed software packages.

VM Attacks

- Once a VM is **compromised,** the attacker has access to the shared resources of that VM.

Back
Next
Back to Main

Virtualization Security

Hypervisor Attacks

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

Common Threats

Data Breaches

- Cloud computing has **widened the scope** for data breaches
  - Multitenancy
  - **Shared** databases
  - Multiple locations
  - Key management
  - Widely dispersed attack surface
- Increase in **smart devices**
  - **Lost** devices
  - Can by difficult to manage **(BYOD)**
  - Laptops/tablets replacing desktops
- In the event of a **sensitive data** breach, companies may:
  - Need to publicly **disclose** the breach (lose credibility)
  - Pay **fines**
  - Lose the ability to legally process certain types of data

Data Loss

- Loss of information by **deletion, overwriting, corruption, of loss of integrity**
- Items to consider in the cloud with respect to data loss:
  - Is the CSP responsible for **backups**?
  - If so, are they responsible for all data or only some?
  - What is the process for **restoring** data?
  - On a shared platform, such as an application, can a **single customer's data** be restored? (SaaS)
- Remember: If you **lose an encryption key** and can no longer decrypt and use data, it's considered lost!

Common Threats

Account or Service Traffic Hijacking

- Frequently done via social engineering attacks **(phishing)**
- May sniff insecure data to capture credentials
- May **pose as a third-party** vendor (trusted entity)
- **Awareness is key** for prevention
- MFA should be used on all public-facing services

Insecure Interfaces and APIs

- Application programming interfaces (APIs) are used to **interact** with cloud services via a command or script.
- APIs must follow **security policies** and not act as a back door.
- All API updates must be scrutinized and **validated** for security 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**
- **Distributed Denial of Service (DDoS)** attacks are launched from multiple locations against a single target (hard to stop)
- Work to **reduce single points of failure**

Common Threats

Malicious Insiders

- Intentional **misuse of access** to data, which affects the confidentiality of the data
- Could be a current or former employee, contractor, or other business partner

Abuse of Cloud Services

- Attackers can use cloud services too, if they're willing to pay.
  - Dictionary attacks
  - **DoS attacks**
  - Password cracking
- CSPs watch for **nefarious activities**, especially DoS/DDoS attacks.

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 that help protect the company from threats
- As cloud security professionals, we should consider:
  - A CSP's **security practices**
  - If your CSP were to close, are you poised to quickly change CSPs?
  - Always have an **exit strategy.**

Common Threats

Shared Technology Vulnerabilities

- Vulnerabilities of hardware, OSes, and apps are shared in shared environments, meaning they **affect all users.**
- CSPs should use a **defense-in-depth** strategy, which implements controls at each layer:
  - Compute
  - Storage
  - Network
  - Application
  - User security enforcement
  - Monitoring

OWASP Top 10

OWASP Top 10 Mapping 2016

	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: Verify for Security Early and Often	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C2: Parameterize Queries	✓									
C3: Encode Data	✓		✓							
C4: Validate All Inputs	✓		✓							✓
C5: Implement Authentication Controls		✓								
C6: Implement Appropriate Access Controls				✓			✓			
C7: Protect Data						✓				
C8: Implement Logging and IDs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C9: Leverage Security Frameworks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C10: Error and Exception Handling	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

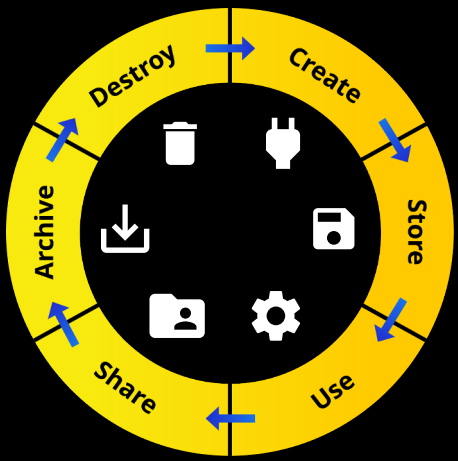
Back
Next

Back to Main

Cloud Security Data Lifecycle

Data is the most valuable asset for most organizations.

Data should be managed across a lifecycle, which includes the following **6 phases:**



It's very importance to ***always*** know where your data resides!

Next

Cloud Security Data Lifecycle (Cont.)

Data Governance Terms

- **Information Classification:** Description of valuable data categories (confidential, regulated, internal only, etc.)
- **Information Management Policy:** What activities are allowed for different information classifications
  - Sensitive data cannot leave premises
  - Regulated data cannot be copied to external media
- **Location and Jurisdictional Policies:** Where data can be geographically located and any regulatory or legal concerns
- **Authorization:** Who is permitted to access different types of data
- **Custodianship:** Who is responsible for managing specific data

Cloud-Based Disaster Recovery & Business Continuity

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 **at least annually.**

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 equally important.
  - Revenue-generating services rank higher.

BCM and **DRP** combine to make **BCDR.**

Cloud-Based Disaster Recovery & Business Continuity

Critical Factors for Business Continuity (BC) in the Cloud

- Understand who the **responsible party** is.
  - Customer's responsibilities
  - CSP's responsibilities
  - Third-party responsibilities (application vendors)
  - **Order** of restoration
  - Right to **audit** CSP capabilities for validation
  - Communication of any issues
  - Need for a **tertiary backup** at another location
- Document in the SLA what BCDR is handled by CSP and to what degree.
  - **Penalties** for loss of service
  - Recovery Time Objective **(RTO)**/Recovery Point Objective **(RPO)**
  - Loss of integrity
  - Points of contact and **escalation process**
  - **Failover** capabilities and process
  - Communication of changes being made
    - Maintenance and upgrades
  - **Clearly defined** responsibilities
  - Where third parties are being used by the CSP

Cloud customers should be **fully satisfied** with the BCDR details prior to signing any agreements.

- Future modifications may result in **additional charges.**

Cloud-Based Disaster Recovery & Business Continuity

Important SLA Components

- No undocumented **single points of failure**
- **Migration** to another CSP should be permitted within an agreed-upon time frame
- Customer should be able to **verify data integrity** via automated controls
- Data **backup solution** should allow for granular settings

Regular reviews of the SLA should occur to ensure cloud services continue to meet the needs of the business.

Cost-Benefit Analysis

Cost is usually a key factor in deciding to move to the cloud.

Cost Considerations

- **Resource pooling:** CSPs offer pooled resourced, which can help keep costs down.
- **Shift from CapEx to OpEx:** Why not pay as you go instead of making a large upfront investment?
- **Time and efficiency:** Cloud is easy to manage and has many automation capabilities built in.
- **Avoid depreciation:** With the cloud, there are no company-owned assets to depreciate off the books.
- **Reduced maintenance:** CSPs handle a large portion of required maintenance.
- **Focus:** The cloud allows organizations to focus on their business with less labor to manage the cloud environment.
- **Utility costs:** Avoid/reduce on-premises electricity and cooling costs.
- **Software and licensing costs:** CSPs can provide great pricing on licensing, as they buy in bulk.
- **Pay by usage:** Only pay for resources used in the cloud; ability to track usage and bill internal departments.

Other things to **consider** when calculating **Total Cost of Ownership (TCO)**:

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

Functional Security Requirements

- **Functional requirements** are services required for a person or the business to accomplish a job.
- **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** are a ***must*** to avoid this!
- **Interoperability**
  - Ability of a cloud service customer to **interact** with cloud services and for cloud services to interact with each other
  - **Avoid** proprietary formats and technology
  - Regularly **review** requirements (business, legal, operational)
- **Portability**
  - Ability for a cloud service customer to easily **migrate** data between cloud service providers
  - Ensure **favorable** contract terms for portability
  - Have an **exit strategy** from day one
  - **Avoid** proprietary formats and technologies

Security Considerations for Different Cloud Categories

Security Considerations for IaaS

- Controlling network **access**
  - Using **security groups** to open & close ports/protocols
  - 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 VMs

Security Considerations for SaaS

- **Access control** to applications
  - Secure passwords & MFA
  - Account lockout & notification
  - VPN access
- Controlling devices where application is accessed **(BYOD)**
- **Monitoring** for availability, security, and audit purposes

Security Considerations for PaaS

- System and resource **isolation** (due to multitenancy)
- **Access** control
- **Secure coding** practices for in-house applications
- **Monitoring** for availability, security, and audit purposes
- Protection against **malware**

Security Considerations for All Cloud Categories

- Know **where** your data is
- **Review contracts and SLAs** so you know what to expect
  - What services you are guaranteed
  - What turnaround time is for requests
  - What **BCDR services** are available and agreed upon

Verification Against Criteria

Key Point: If it cannot be measured, it cannot be managed.

- How do you know if something is meeting **standards** if you have no **data** to validate against?

How can we evaluate cloud vendors effectively? Surely there's a **tool** out there that can help with this.

Cloud Certification Schemes List (CCSL)

- Created by the European Union Agency for Cybersecurity (ENISA)
- Provides an **overview** of different cloud certification schemes (certifications) and shows the main characteristics of each scheme. It also answers questions such as:
  - Which 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 of 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
- Basically a **checklist** explaining each scheme (certification) to help you better **understand** each one.

Verification Against Criteria (Cont.)

Cloud Certification Schemes Metaframework (CCSM)

- Created by the European Union Agency for Cybersecurity (ENISA).
- The **other half of CCSL.**
- Allows users to **select** their security objectives, then suggests **schemes** (certifications) containing these objectives for users to review.
- To access this framework and view different schemes, use the **CCSM Online Procurement Tool**.

CSA Security, Trust, and Assurance Registry (STAR)

- Created in 2011 in response to the need for a **single consistent framework** by which to evaluate vendors
- STAR is managed by the **Cloud Security Alliance (CSA)**
- There are **2 parts** to STAR (like with CCSL/CCSM):
  - **Cloud Controls Matrix (CCM):** A list of security controls and principles for the cloud environment
  - **Consensus Assessments Initiative Questionnaire (CAIQ):** A self-assessment performed by the CSP **(self-audit)**
- There are **3 levels** of STAR certification:
  1. **Self-assessment:** Fill out the CAIQ
  2. **CSA STAR attestation:** Third-party audit
  3. **Continuous auditing:** Using the CloudTrust Protocol

CloudTrust Protocol: CSP agrees to **openly share** certification information with customers and prospective customers.

Verification Against Criteria (Cont.)

- **ISO 27001:** Most widely known and accepted information security standard. ISO 2700:2013 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: Auditor findings at a **point in time**
    - Type 2: Operational effectiveness **over time**
  - **SOC 2:** Meant for **IT service providers and cloud providers**
    - Addresses the five Trust Services principles (Security, Availability, Processing Integrity, Confidentiality, Privacy), providing a detailed technical report.
    - Also uses **Type 1 & 2** reports like SOC 1.

Verification Against Criteria (Cont.)

SOC 1 / SOC 2 / SOC 3 (Cont.):

- **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 a SOC 2 report would.
- **SOC reports** are performed in accordance with **Statement on Standards for Attestation Engagements (SAE) 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; a **risk management framework.**

PCI DSS: A security standard by which all organizations that accept, transmit, or store **credit card data** must comply.

- There are 4 merchant levels based on the number of annual **transactions;** used to determine the level of compliance required.
- Processors are to **never store** the card verification (CVV) number.
- Failure to comply can result in **severe fines** and the **loss of authority** to process credit card transactions.

System & Subsystem Product Verification

Why do we need to ensure CSPs are certified?

- Our data resides with the CPS and we **trust** them to protect its confidentiality, integrity, and availability (CIA).
- Cloud vendors who meet standards criteria are more likely to provide us with the **CIA** we require, which reduces risk.
- Imagine using a cloud vendor with no certifications.
  - We know nothing about their **capabilities.**
  - No third-party **audits** have taken place to validate anything.
  - Trusting this vendor would be a **high-risk decision.**

Common Criteria (CC) Assurance Framework (ISO/IEC 15408-1:2008)

- International standard designed to **provide assurances** for security claims by vendors
- Primary goal is to **assure customers** that products have been thoroughly tested by third parties and meet the specified requirements.
- **https://www.iso.org/standard/50341.html**

- CC has **two key components:**
  - **Protection profiles:** A standard set of security requirements for a specific type of product such as a firewall, IPS, switch, etc.
  - **Evaluation Assurance Levels (EALs):** Define how thoroughly the product is tested (scale of 1-7).
    - **1 = Lowest; 7 = Highest**

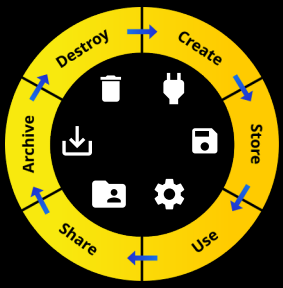
System & Subsystem Product Verification

FIPS 140-2

- A NIST document that lists accredited **cryptosystems**
- The **benchmark** for validating the effectiveness of cryptographic hardware and systems
- All cryptosystems used should meet FIPS 140-2 compliance
- Check to ensure your CSP is **FIPS 140-2 validated**

- FIPS compliance is measured on a scale of **1-4.**
  - **Level 1** is the **lowest**.
  - **Level 4** is the **highest** level of compliance and indicates the product provides the **highest level of security.**

Lifecycle Phases



Cloud Data Lifecycle Phases

- **Create:** The creation, acquisition, or altering of data. Preferred time to **classify data**.
- **Store:** Committing data to storage. At this point, implement **security controls** to protect data (encryption, access policies, monitoring, logging, and backups).
- **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 during this phase.
- **Share:** It's difficult to manage data once it leaves the organization. **DLP and IRM** can be helpful for managing what data can be shared.
- **Archive:** Moving data that is no longer actively being used to **long-term storage**. Archived data must still be protected and meet regulatory requirements.
- **Destroy:** Removal of data from a CSP.

Back
Next

Back to Main

Lifecycle Phases (Cont.)

Three Key Data Functions

- **Access:** Viewing and accessing data
- **Process:** Use of data to perform a function
- **Store:** Storing data in a database or filesystem

Controlling Data Functions

- **Access:** How do we control access?
  - Access management **(access lists)**
  - Encrypt data
  - Digital rights management (DRM)
- **Process:** How do we control processing?
  - Access management
  - Data **encryption**
- **Storing:** How do we control the storage of data?
  - **Policies** are a start
    - How certain types of data are stored
    - USB restriction policies to prevent USB storage
  - DRM to prevent copying of data
  - **Data loss prevention (DLP)** solutions
    - Can enforce rules and prevent data from being moved or copied

Encryption

Access Control

Data Dispersion

Location
- Data **moves** between locations
- Services **replicate** data across geographic regions
- Important data should **always** be stored in multiple locations

Storage Slicing (data dispersion)
- Data is **broken into chunks** and encrypted, error correction **(erasure coding)** is added, and then data is geographically distributed
- Allows for retrieval of data in the event **multiple locations** are offline
- Like **RAID** for the cloud

Automation
- Automated **dispersal** of data
- Data dispersion policies are critical
  - Ex: **Intellectual property (IP)** cannot leave the US
  - **Accidental** replication of TBs of data is costly

IaaS
- CSPs offer different **classes of service** that automatically replicate data across geographically dispersed locations

PaaS/SaaS
- **Research** prospective providers to ensure they practice data dispersion
- May be an additional feature **not enabled by default**
- May incur additional **costs**

Back
Next

Back to Main

Storage Types

IaaS

- **Volume:** Virtual disk attached to a virtual machine (Ex: VMFS, AWS EBS)
- **Object:** Storage pool, like a file share (Ex: AWS S3)
- **Ephemeral:** Temporary storage used while a system is up and running. Once the system is shut down, the storage goes away.
  - Temporary storage
  - **Pagefile**

PaaS

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

Other Storage Types

- **Raw Storage**: **Raw device mapping (RDM)** is an option with VMware virtualization that allows you to map directly to physical storage such as a LUN.
- **Long-Term**: Data archiving services such as AWS Glacier.
- **Content Delivery Network (CDN)**: Files are stored in geographically dispersed object storage; used to improve the user experience by speeding up delivery to consumers.

Threats to Storage Types

Unauthorized Usage and Access
- Cause: Account **hijacking** or lack of access controls
- Solution: **Multi-factor authentication (MFA)** and secure access controls

Liability Due to Regulatory Non-Compliance
- Cause: **Missing** requirements and lack of internal auditing
- Solution: **Implement** regulatory requirements and regularly **self-audit**

Denial of Service (DoS/DDoS) Attack
- Cause: **Lack** of edge security
- Solution: **Implement** security products (such as an IPS) to prevent DoS/DDoS attacks

Corruption, Modification, and Destruction
- Cause: Human or mechanical **error**
- Solution: Ensure **backups** are functional, regularly test

Data Leakage and Breaches
- Cause: **Holes** in security (weak patching, access controls, etc.)
- Solution: **Data loss prevention (DLP)** products, **penetration tests**

Back
Next
Back to Main

Threats to Storage Types

Theft or Loss of Media
- Cause: **Unencrypted** data being lost or stolen
- Solution: **Encrypt** data at rest (laptops, mobile devices, USB devices, etc.)

Malware Introduction or Attack
- Cause: Most likely **human error**
- Solution: Security **training** and security products (anti-virus, anti-malware, etc.), network **segmentation**

Improper Treatment or Sanitization After End of Use
- Cause: Data not being deleted **properly**
- Solution: 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

Crypto-Shredding
1. Encrypt data with key A.
2. Encrypt key A with key B.
3. Delete data.
4. Delete key A and key B.

Threats to Storage Types

Data responsibility

- The client is **ultimately responsible** for the safeguarding of sensitive data (PCI, PII, HIPPA, etc) from cradle to grave
- Even if the data disclosure is the **fault of another party**, the client is still ultimately responsible

Cloud Data Security

Data Security Technologies & Strategies

Encryption & Key Management

Implementing Encryption at Different Points

- **Data in motion (DIM):** IPSec can be used via **VPN**; **SSL & 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 (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 process
- **Encryption keys:** Values used during the encryption process that are later used to decrypt the data

Challenges for Encryption in the Cloud

- Key management is **paramount**. Whether the key resides in the cloud or on premises, it must be protected.
- Issues may arise if the CSP needs to **process** the encrypted data.
- **Multitenancy** uses shared resources such as **RAM,** where encryption keys could reside temporarily.
- CSPs mostly offer **software-based encryption,** which is more vulnerable than hardware-based encryption.
- Encryption can impact **performance.**
- Be wary of solutions that use a **proxy type** encryption engine, as it can be a single point of failure.
- Data **integrity** can be compromised with file replacement attacks. May need to use **digital signatures** on files.

Encryption & Key Management (Cont.)

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 mounted to a **virtual machine** (VM).
  - Does not protect against access through the operating system, such as attackers or rogue employees
  - Two methods to implement:
    - **Instance-based:** Encryption engine resides on the VM instance.
    - **Proxy-based:** Encryption engine runs on a proxy instance. The proxy maps the volume data to the instance for secure access.
- **Object storage encryption:** Basic storage-level encryption is less secure, so it's best to encrypt data before sending it to the cloud.
  - **File-level encryption:** Using an IRM or DRM solution to protect individual files.
  - **Application-level encryption:** The encryption engine resides within the application itself, allowing the application to ingest and use encrypted data.
- **Database encryption:**
  - **File-level encryption:** (See above)
  - **Transparent encryption:** Encryption engine resides within the database itself.
  - **Application-level encryption:** (See above)

Encryption & Key Management (Cont.)

Key Management

- The **most challenging** component of encryption
- Common challenges with encryption keys:
  - **Access to keys:** Regulatory requirements and ensuring CPSs don't have access
  - **Key storage:** Keys 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 be transmitted in plain text.
- 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 VM or application where the encryption engine resides.
  - **Protects against** data loss
- **Externally managed:** Keys are stored separately from the encryption engine and data.
  - Must consider how key management is integrated with the encryption engine (more complicated)
- **Managed by a third party:** Key escrow services

Encryption & Key Management (Cont.)

Key Management in Software Environments

- CSPs normally use software-based encryption to **avoid costs** associated with hardware-based encryption.
  - Software-based encryption is **more vulnerable** to exploits than hardware-based encryption.
- Software-based encryption **doesn't meet** NIST's FIPS 140-2 or 140-3 specifications.
  - Software-based encryption has a hard time identifying signs of **tampering.**
  - May cause an issue if you work with US federal government agencies.
- It's **your responsibility** to find out what type of encryption your CSP offers.

Data Encryption

Cloud Data Security

Data Security Technologies & Strategies

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 *cannot* be used to **reverse-engineer** the original data

Back

Next

Back to Main

Masking and Obfuscation

- **Masking and data obfuscation:** 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** such as SSN, DOB, phone number, etc.
- Sometimes used to take production data and turn it into **testing data** by masking sensitive data
- **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:** Uses "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 **on the move** between storage and use

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.

Benefits of Tokenization

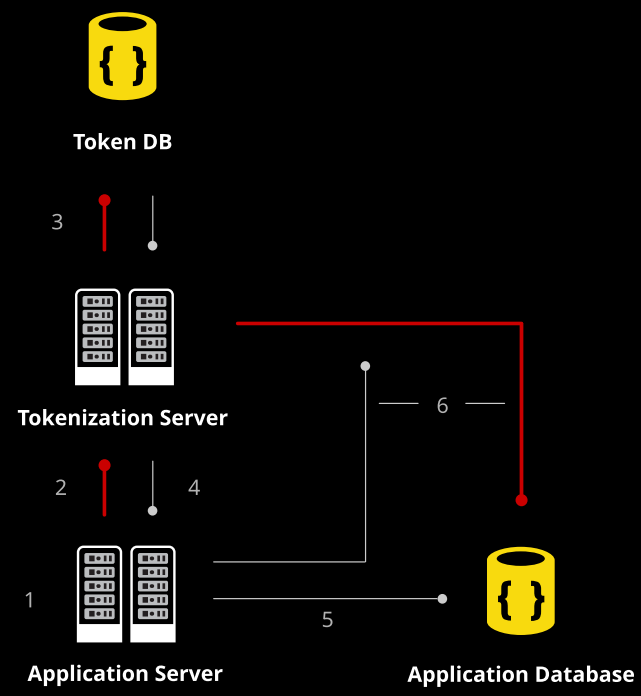
- **Complying** with regulatory requirements
- Reducing the **cost** of compliance
- Reducing the **risk** associated with storing sensitive data
- Reducing the **attack vectors** of sensitive data

6 Steps of Tokenization

1. Sensitive data is **generated.**
2. Data is **sent** to the tokenization server.
3. A token is generated, and the sensitive data and its associated token are **stored** in a database.
4. The tokenization server sends the token back to the application so it can **substitute** the sensitive data with it.
5. The application **stores** the token.
6. When sensitive data is needed, the data can be requested by the application by **submitting** the token.

Tokenization Diagram

Tokenization



Back

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 **watch 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**
- Is **not** considered to help with access control

DLP Components

- **Discovery and classification** (what to look for)
- **Monitoring** (notification of issues)
- **Enforcement** (prevent data loss)

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 identifying data as it's installed on the system where the data resides; generally needs another mechanism for enforcement.
- **Data in use (DIU):** Client- or **endpoint-based**. Resides on users' workstations. Requires a considerable amount of management; not easy to deploy and manage.

Data Loss Prevention (DLP) (Cont.)

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 **hardware** solution would need approval to be racked at the datacenter and would be difficult to get approved
  - If it's a **CSP offered** product, no worries!
  - If it's software your deploying into **PaaS**, no worries!
  - If it's a virtual image deploying 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 **(geographically)**?
- How should the data be stored **(encrypted)**?
- When can data **leave** the cloud, if ever?

Most cloud vendors offer DLP solutions. If yours doesn't, there are many commercial offerings.

Data De-Identification (Anonymization)

Anonymization: The process of removing direct and indirect identifiers.

- Can be done by sampling like data and **generalizing the data** to ensure the group shares the same value for sensitive data.
- This would make it **hard to identify** a single individual because the sensitive data is the same for all users.
- Think ***Where's Waldo?*** but with data.

Example Scenario

- In a system, there is a list of home **addresses.** If all the addresses were grouped by ZIP code, it would **make it difficult** to pick out a single person who lives in Baltimore because 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.). 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.

Cloud Data Security

Data Discovery and Classification

Structured and Unstructured Data

What Data Do We Have?

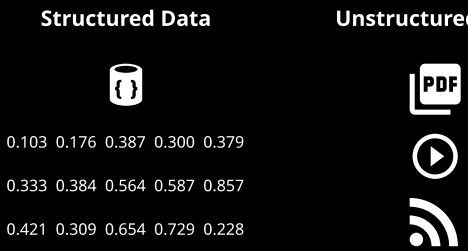
- If we don't already know, we need **data discovery.**
- Maybe we already know, but we want to get more out of it.

Data Discovery

- Can have more than one meaning
- Working to create a **data inventory**
- E-discovery is the process used to collect **electronic evidence** for a criminal investigation
- Collection and **analysis** of data 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)



Cloud Data Security

Data Discovery and Classification

Structured and Unstructured Data (Cont.)

Data Discovery Approaches

- **Big Data:** Analyzing very large data sets to extract information
- **Real-Time Analytics:** Looking for patterns of usage
- **Agile Analytics:** Free-form adaptive analysis that focuses on a specific need and doesn't look all data
- **Business Intelligence:** Analyzing data and presenting useful information to help decision makers

Data Discovery Techniques

- **Metadata:** Information about a file (owner, size, creation date, etc.)
- **Labels:** Labels assigned to data by the owner
- **Content Analysis:** Analyzing data content using keywords

Data Discovery Issues

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

Challenges with Data Discovery in the Cloud

- Can be hard to identify **where the data is** (dispersed/replicated)
- Accessing the data can be tricky

Cloud Data Security

Data Discovery and Classification

Mapping, Labeling, and Sensitive Data

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 by the organization when classifying data
- Data **owners** will apply labels to adhere to the classifications

Classifications

- Confidential, **Secret,** Top Secret
- **Internal only**, limited sharing

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

Labeling: Tags applied to data by the data owner that describe the data.

- **Common labels:**
  - **to encrypt,** not to encrypt
  - internal use, **limited sharing**
  - **sensitive**

Sensitive Data

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

Cloud Data Security

Information Rights Management

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?*
- **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 up to their **discretion.**

Objectives (Cont.)

IRM Challenges in the Cloud

- Each individual resource must be provisioned with an access policy **(heavy management)**
- Each user must be provisioned with an account and keys (consider **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

Information Rights Management

Appropriate Tools

Capabilities and Tools of IRM Solutions

- These tools are **features** of an IRM solution
- Persistent **protection** 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**

Cloud Data Security

Data Retention, Deletion, & Archiving Policies

Retention Policies

Data retention policies should contain the following:

- **Retention periods: How long** to keep the data
  - Will be based on legal and regulatory **requirements**
  - **PCI Requirement 3.1:** Organizations should "Keep cardholder data storage to a minimum"
  - **HIPAA:** Requires some data to be retained for 6 years
  - **IRS:** 7 years, in some cases
  - What are **your organization's** data retention requirements?
- **Retention formats:** What type of media is used, is it encrypted, and what is the retrieval process?
- **Data classification:** How specific data classifications will be stored and retrieved
- **Archiving and retrieval procedures:** Detailed instructions on these processes
- **Policy review and enforcement:** How often the policy will be reviewed for effectiveness and who will be responsible for enforcing the policy

AWS Config

- Service that allows you to **assess, audit, and evaluate** the configs of your AWS resources
- Provides the ability to create **retention policies** for data and will auto-delete data based on policy rules

Check to see what your CSP offers, or ask prospective CSPs what they offer!

Cloud Data Security

Data Retention, Deletion, & Archiving Policies

Deletion Procedures & Mechanisms

In the Legacy Environment
- Physical **destruction** of hardware
- **Degaussing**
- Overwriting with multiple passes
- **Crypto-shredding**

Cloud Data Deletion
- **Crypto-shredding** is the best option

Crypto-shredding
1. Encrypt data with key A.
2. Encrypt key A with key B.
3. Delete data.
4. Delete key A and key B.

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

AWS Data Sanitization Procedures
- AWS uses techniques outlined in **NIST 800-88** (*Guidelines for Media Sanitization*) when decommissioning customer data
- **Amazons EFS (Elastic File System)** is designed such that once data is deleted, it will never be served again

Cloud Data Security

Data Retention, Deletion, & Archiving Policies

Archiving Procedures & Mechanisms

- **Data archiving:** The 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 archived data
  - Backup and DR options if any archived data is necessary for **business continuity (BC)**
  - A record of the data **format**, as proprietary formats may change over time (MS Office 98 documents may be impossible to open in a newer MS Office version)
  - Detailed data **restoration procedures**

- **Example: AWS Glacier** can be used for archiving data
  - Archival storage **may not be acceptable** for BC/DR purposes because they are often **slow to retrieve data** and will impact recovery time objectives (RTOs)

Archiving Procedures & Mechanisms Cont.

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 resides
  - Will the media deteriorate over time

Back
Next

Back to Main

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

Legal Hold Options in AWS

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

Cloud Data Security

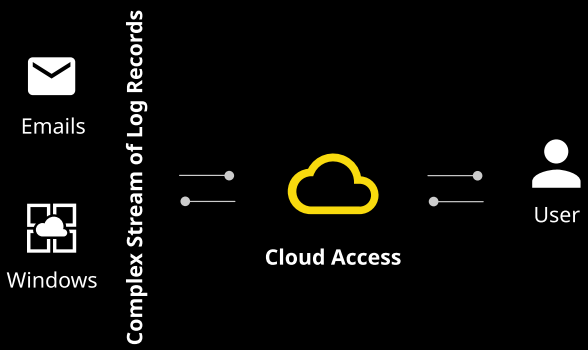
Auditability, Traceability & Accountability of Data Events

Event Sources & Requirements

Event sources: Systems, services, or devices that create and provide log events for analysis

SaaS Event Sources

- Typically have **minimal access** to event data
- Will most likely only be high-level application log data generated 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



Event Sources & Requirements (Cont.)

PaaS Event Sources

- Since the organization is developing on the PaaS platform, the organization's **development team** will need to be consulted 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, permissions 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.)

Cloud Data Security

Auditability, Traceability & Accountability of Data Events

Event Sources & Requirements (Cont.)

IaaS Event Sources

- Should have **access to** event and diagnostics data
- Many of the **infrastructure logs** will be available
- Logs that 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/version)
  - IP addresses
  - **Service name**
  - URL or code information
  - **Accounts** involved
  - **Severity**
  - Description

AWS offers **Centralized Logging** (built on the Amazon Elasticsearch service), which allows for **collection and analysis of AWS service logs.**

Cloud Data Security

Auditability, Traceability & Accountability of Data Events

Logging, Storage & Analysis

Security Information & Event Management (SIEM)

- SIM + SEM = 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

SIEMs provide:

- **Data aggregation:** Bringing many logs from the operating system, network devices, and applications together for analysis
- **Correlation:** Looking for common attributes within the logs that can be used to link events together
- **Alerting**
- **Dashboards:** Much **faster** than reading through reports
- **Compliance:** Can generate **compliance reports** based on event log data
- **Retention:** Long-term storage
  - Most SIEMs don't actively provide long-term storage. They tend to **offload events** after a certain age to an internal archival area. This is because 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

Chain of Custody & Non-Repudiation

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

Documentation Requirements

- When evidence was **collected**
- Where evidence is **located, during which dates,** and who placed it there (for storage of evidence)
- **Transfer** of evidence (from whom to whom, when)
- **Access** to the evidence
- **Analysis performed** on the evidence

A **chain of custody form** should be used to document the transfer of evidence between individuals.

Chain of Custody Form

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

Non-repudiation: 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)

Chain of Custody & Non-Repudiation

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

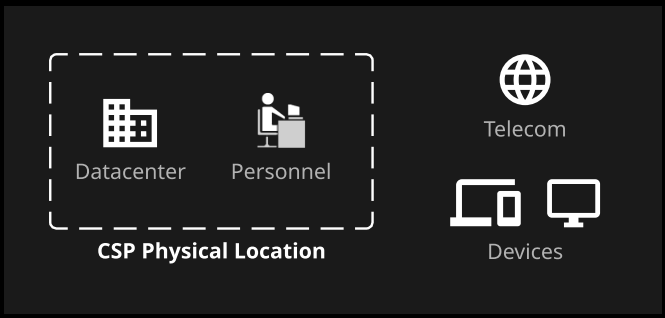
Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Chain of Custody Form

Back

Cloud Infrastructure Components

Physical Environment



Shared responsibility: The idea that the CSP is not wholly responsible for security; instead, it is a **shared responsibility** between the customer and the CSP.

- In IaaS, the CSP is **not** responsible for:
  - Patching customer VM **operating systems**
  - Installing and managing security endpoint solutions
  - Managing **access lists** in the customer's environment
  - Compliance of settings the customer chooses to use
- In PaaS, the CSP is **not** responsible for:
  - Ensuring the customer **follows** secure coding practices
  - Compliance of the customer's **code**
- In SaaS, the CSP is **not** responsible for:
  - Compliance with how the customer **uses** the software
  - The type of data the customer enters into the software

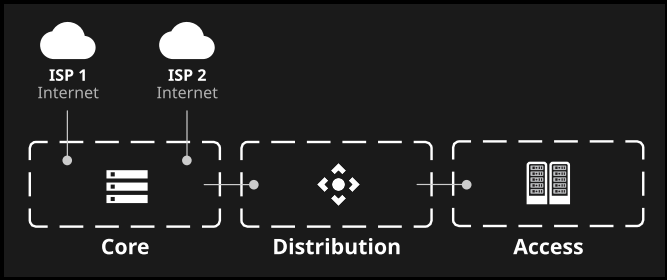
Back

Next

Back to Main

Cloud Infrastructure Components

Network and Communications



- Remember, cloud data still runs on **hardware!**
- **Cloud carrier:** Organization that provides connectivity between the CSP and the cloud customer.
- **Network Functionality**
  - Address **allocation** (DHCP)
  - Access **control** (IAM)
  - Bandwidth allocation: **Reserving** bandwidth for a specific use
  - **Rate limiting:** Limiting the amount of traffic
  - Filtering: Closing ports or **blocking** specified protocols
  - **Routing**
- **Software-Defined Networking (SDN):** Allows for networking to be completely **programmable,** and the underlying hardware is simply commodity hardware. The goal is to make networking more **agile, flexible, and centrally managed.**

Back

Next

Back to Main

Cloud Infrastructure Components

Compute

- Compute capacity is **dependent on:**
  - Number of **CPUs**
  - Amount of **memory**
- **Reservation:** A guaranteed minimum amount of resources allocated to a guest (VM)
- **Limits:** Maximum amount of resources allocated to a guest (VM)
- **Shares:** Each guest is assigned a number of shares, and when contention occurs, those shares determine the amount of the available **resources** that a guest receives

Back

Next

Back to Main

Virtualization

- **Virtualization**: Includes the use of compute, storage, and network
- **Capacity monitoring:** Used to ensure that **resource allocation** to the tenants of the virtual environment is fair and policy-based.
- Sharing **resources** enables more efficient use of hardware
- Virtualization allows for **easier management**
- **Hypervisor**: Software, firmware, or hardware that makes a guest OS think it is running directly on physical hardware.
  - Allows for running **multiple** guests on the same hardware
  - Two types of hypervisors:
    - **Type 1:** Bare metal, runs directly on hardware
      - Ex: VMware ESXi
    - **Type 2:** Runs on top of another OS
      - Ex: VMware workstation or VirtualBox
      - **More susceptible** to vulnerabilities and exploitation
  - **Risks** associated with hypervisors:
    - Vulnerabilities in the hypervisor can lead to **guest targeting**
    - **VM hopping:** One tenant is able to see another tenant's data
    - Resource **starvation** in high-contention times
    - **File** attacks on images or snapshots

Storage

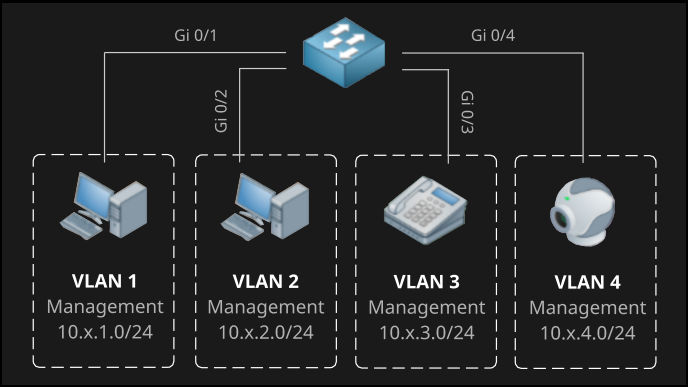
- **Primary** method of protecting data at rest is encryption
- **Block Storage**
  - Primary **role** of storage is to group disks together into logical volumes (LUNs, virtual disks, generic volume storage, and elastic block storage)
  - Does not have a **file system** when created
  - It's up to the **OS** on the VM to create the file system
- **Object Storage**
  - Has a flat **file system** already on it
  - **Simple** file storage (files of nearly any type)
  - Objects available via **browser and REST API**
  - Examples:
    - **AWS S3**
    - **Rackspace Cloud Files**
  - Typically the best way to store an **OS image or snapshot**
  - Data can be **replicated** across multiple stores
- **Things to remember about object storage:**
  - Takes **time** for changes to replicate
  - **Not good for** real-time data collaboration
  - **Best for** static objects
  - **Good for** backup storage, images, other static files

Management Plane

- Controls the **entire infrastructure** and is very **high-risk**
- Allows admins to remotely manage **all hosts**
- **Key role** is to create, provision, start/stop VM instances and live migration of VMs.
- **Customers** have partial access via:
  - **Web** portal
  - **Command line** interface
  - **APIs**
    - All of these must have **strict** access controls
- Regulatory requirements may call for a **physically separate network**
- 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

Logical Design

- Datacenters provide many basic services, known as **"Power, Pipe, and Ping"**
  - **Electrical power**
  - **Air conditioning**
  - **Network connectivity**
    - Power and pipe limit the **density** of servers in a datacenter
- **Multitenancy**
  - Must securely segregate tenants
  - Logically separated physical networks (Ex: VLANs)



Logical Design (Cont.)

- **Cloud Management Plane**
  - Provides 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 implemented solutions must provide an **acceptable level** of audit capabilities
- **Automation**
  - **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**

Logical Design (Cont.)

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** capabilities
- **Retention** periods
- **Reporting** capabilities

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 regulatory requirements ahead of time

Physical Design Standards

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

Size

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

Back

Next

Back to Main

Physical Design (Cont.)

Design Considerations

- Protection against **natural disasters**
- **Access** to resources during a natural disaster
  - **Telecommunications**
  - **Clean water**
  - **Clean power**
  - **Accessibility** (not too remote)

Physical Protection

- Fences, walls, gates
- Electronic **surveillance**
- Ingress and egress **monitoring**

Buy or Build

- Datacenter **tier certification**
- Physical **security**
- **Usage** (dedicated vs. multitenant)
  - Significant investment either way

Datacenter Design Standards

- **Building Industry Consulting Service International (BICSI) | ANSI/BICSI 002-2014:** 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 & 76:** Specify how hot or cold aisle containment should be. **NFPA 70:** Requires implementation of an emergency power-off button to protect first responders.

Physical Design (Cont.)

Uptime Institute Data Center Site Infrastructure Tier Standard

Topology:

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

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

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 equals **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 datacenter

- **Air Management**
  - Work to **prevent** the mixing of incoming cool air and hot air exhaust
  - Prevents heat-related **outages**
  - **Reduced** 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**

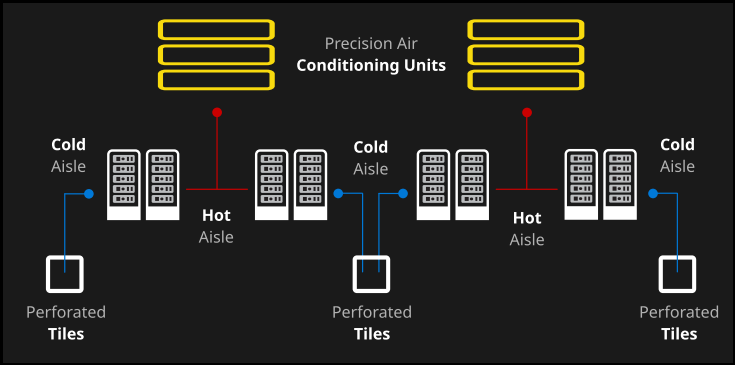
Environmental Design (Cont.)

Cable Management

- Minimize airflow **obstructions**
- **Raised-floor** environments should have 24 inches of clearance
- **Cable mining** program
  - **Ongoing** cable management plan
- Key factor in 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
- Requires hardware to be installed in the **proper direction**
- **Plastic sheeting** may be used to separate cold aisle

Environmental Design (Cont.)

Aisle Separation and Containment (Cont.)

- Empty U's in rack should be 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

Environmental Design (Cont.)

HVAC Design Considerations

- **Local climate** will affect HVAC designs
- **Redundant** HVAC should be used
- HVAC design should include keeping cold and warm air **separate**
- Ensure **backup power** is calculated for HVAC
- HVAC should **filter** contaminants and dust

Multi-Vendor Pathway Connectivity

- **Redundant** connectivity from multiple internet service providers (ISPs)
- Verify that ISPs use **different backhauls upstream**

Analyze Risks Associated with Cloud Infrastructure

Risk Assessment & Analysis

Types of Risks

- **Policy and organizational** risks: Related to choosing a CSP and outsourcing
- **Provider lock-in**
  - Use **favorable contract language** (best)
  - **Avoid** proprietary data formats
- **Provider lock-out:** Provider is unable or unwilling to provide services (out of business)
  - Keep **data backups** on premises or at another CSP
    - Be careful of **interoperability issues** with different CSP
- **Loss of governance:** Customer is unable to implement all necessary security controls
  - Because they own the underlying infrastructure, cloud providers are **responsible** for defining governance and deploying the necessary security controls; customers have some input, depending on the service model
  - SaaS offers the **least** amount of control over governance
- **Compliance risks:** CSP is unable to provide necessary means for compliance

Risk Assessment & Analysis (Cont.)

General Risks

- Consolidation of services can cause a **small problem to have a large impact** (all eggs in one basket)
- CSPs build complex environments, which require **advanced technical skills**
- **Technical risk** shifts to the provider as they manage the underlying infrastructure
- **Resource exhaustion** due to over-subscription or resource failure

Legal Risks

- **Data protection:** The customer is ultimately responsible for protecting sensitive data such as PII.
- **Jurisdiction:** In the cloud, your data may reside in different jurisdictions, which can **affect regulatory compliance.**
- **Law enforcement:** If a tenant is compelled to hand over data to law enforcement, that tenant could **inadvertently expose** other tenants' 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:** A cloud vendor could try to take ownership of data created in the cloud by stating that it was created on their platform, therefore they own it. Contractual wording should be used to prevent this.

Analyze Risks Associated with Cloud Infrastructure

Cloud Vulnerabilities, Risks, Threats, and Attacks

Cloud-Specific Risks

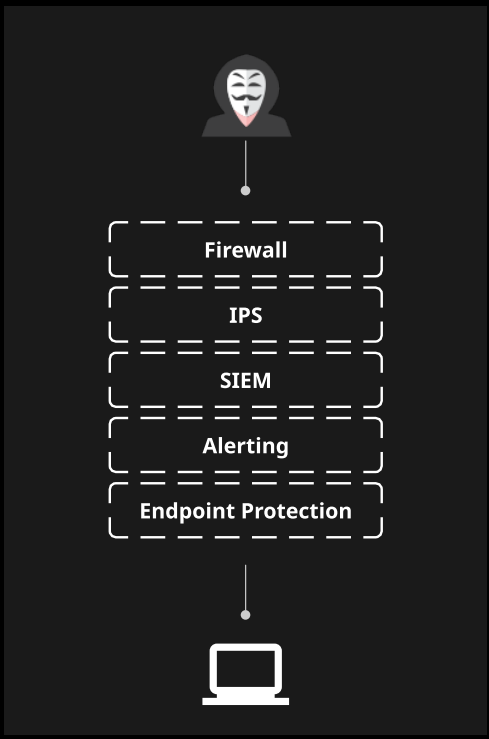
- **Management plane breach:** Serious risk because this would give the attacker access to the entire infrastructure.
- **Resource exhaustion:** Over-subscription by the CSP may result in a lack of resources for your cloud services, which could cause an outage.
- **Isolation control failure:** When one tenant is able to access another tenant's resources or is affecting 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 attack:** Because everything is accessed from a remote location, cloud solutions increase the risk of man-in-the-middle attacks.

Virtualization Risks

- **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 OS, as files are easily moved
- **Sprawl:** Not managing allocation can allow for over-creation of virtual resources

Countermeasure Strategies

Multiple layers of **defense** are needed



Countermeasure Strategies (Cont.)

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 filesystem permissions
  - **Compensating controls** include:
    - Use of **Network Access Controls (NACs)** to prevent unauthorized access to 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

Countermeasure Strategies (Cont.)

Automation

- Use of automation for **configuration**
- Automate the **building of VMs**
  - Ensures they'll all be **up to standards** (updated, patched, use proper security settings, etc.)
  - **Reduces human error** (e.g., forgetting to patch)
  - 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.)

Audit Mechanisms

The **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

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

Audit Mechanisms

- Logs (high-risk events logged)
- Packet captures (prove HTTP authorization denied, only HTTPS accepted)
- Config files
- Policies
- Reports (SIEMs)

Compliance audits need to be conducted by a representative **(regulator)** from the industry or organization that sets the compliance requirements.

Audits of the cloud don't generally involve physical access, so the reports may be **less complete** than an on-premises audit and may be considered **less trustworthy** because of this fact.

Identification, Authentication, and Authorization

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)** 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)

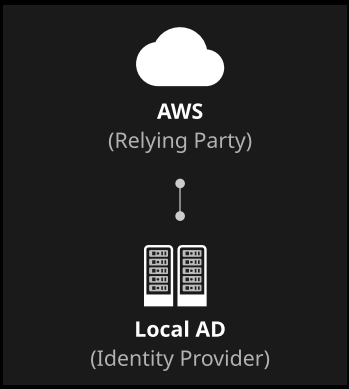
Identity Management
- Authentication done by identity provider
- **Process** of registering, provisioning, and deprovisioning identities

Access Management
- Authorization for relying party
- **Managing** an identity's access rights to resources

Identification, Authentication, and Authorization

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

Ex: Using local Active Directory authentication to log in to AWS.



Identity federation involves two parties:

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

Virtualization System Protection

- **Snapshotting** of images should be considered for incident response and any forensic work that needs to be done
- **Security controls** in virtualization include:
  - Traffic control or **isolation using security groups (access lists)**
  - Guest operating system **security software** (anti-virus, anti-malware, etc.)
  - **Encryption** (file and volume)
  - **Image lifecycle** (image creation, distribution, deletion)

System and Communication Protection (Cont.)

Protecting Data in Motion

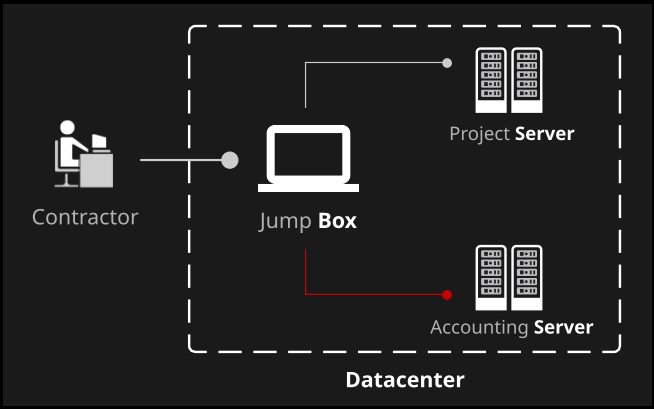
- **VLANs** can be used to separate data, which helps provide data confidentiality and integrity. VLANs also help reduce resource contention and are very often mandated by compliance standards.
- **Encryption** is another way to protect data in motion using:
  - **VPNs** (IPSEC / SSL)
  - **SSL / TLS**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

Data Backups

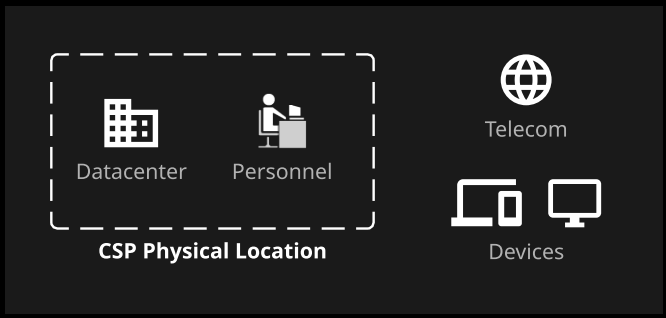
- To the **same CSP** as the production environment
  - Speed up recovery time
- To a **secondary CSP**
  - Avoid provider lock-out

System and Communication Protection

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



Physical and Environmental Protection (Cont.)



Datacenter Protection

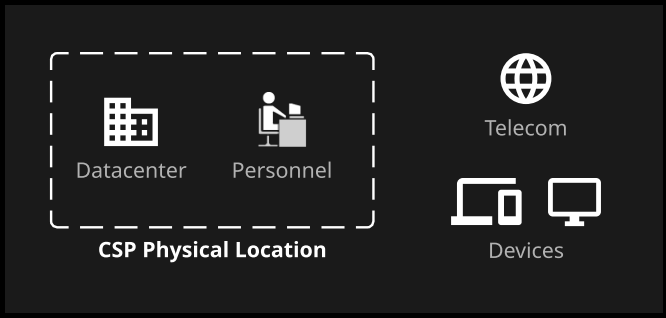
- **Multiple layers**
  - **Guard** at gate
  - Badge **at gate**
  - **Badge** at main door
  - Guard at **main door**
  - **Biometric** check plus badge at each zone with **man trap**

Redundant services (power, cooling, HVAC, networking, etc.)

CSP Personnel

- **Background checks** and screening
- **Training**
- **Incident response**

Physical and Environmental Protection



Physical Security Standards
- **NIST SP800-14:** General principles and practices for securing IT systems
- **NIST SP800-123:** General server security

Key Regulations for 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)

Risks Related to the Cloud Environment

Risks Related to the Cloud Environment

- **Natural disaster** (flooding, power, cooling, damage to physical structure)
- **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 involve high-availability solutions, which are more **complicated** to manage and can be affected by 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

Risks Related to the Cloud Environment (Cont.)

BCDR Scenarios

- **On-premises to CSP failover:**
  - **Technical capabilities** to make this happen
  - **Speed** at which failover can occur
- **Failover between zones within the 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 **vet thoroughly**
  - **Speed** at which the failover can occur
  - **Impact** on end users (will it look different, how do they connect, etc.)

Plan Disaster Recovery and Business Continuity

Business Requirements

- **Recovery Time Objective (RTO):** Acceptable amount of **downtime** for business-critical applications before they need to be functional again after an event
  - **Prioritize** applications and services
  - **If less downtime** is needed:
    - Deploy DR solutions that allow for **faster recovery**
    - **More personnel** to complete tasks

- **Recovery Point Objective (RPO):** Acceptable amount of data the organization is willing to lose if restoration is required after an event
  - Dependent on data **replication schedule**
  - **Ex:** Replication every 4 hours, may lose up to 4 hours' worth of data
  - How to **reduce data loss:**
    - Replicate **more frequently**
      - Increased **bandwidth**
      - **Licensing** costs

- **Recovery Services Level (RSL):** A percentage (0-100%) of the amount of resources (compute) needed during a disaster, based on the services required 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

- **Business Impact Analysis (BIA)** determines the RPO/RTO.

Back

Next

Back to Main

Plan Disaster Recovery and Business Continuity

Business Continuity/Disaster Recovery Strategy

Location

- Is it **far enough** (geographically) from the primary location?
- Is it in a separate **jurisdiction** (compliance)?
- Can the remote site handle the cutover?
  - Adequate **bandwidth and services**

Data Replication

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

Functionality Replication

- **Recreating** the same functions at a different location
- **Passive mode:** Replicated resources are in standby mode
- **Active mode:** Replicated resources are participating in production
- For databases, may use **database as a service** if replicating within the same CSP

Other Considerations

- Replicating to a **second CSP** reduces risk of vendor lock-out with a single CSP
- **Personal safety** is the most important thing
- **Monitoring** is key to failover timeliness

Back

Next

Back to Main

Creating, Implementing, and Testing a Plan

Functional Drill/Parallel Test

- **Mobilize personnel** to other sites
- Establish communications and **perform recovery process** according to BCDR
- **Determine** if critical systems can be recovered at remote sites and BCDR procedures are adequate
- **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 it's an exercise)
- Generally extended over a **longer period of time**
- **Lessons learned,** update plan accordingly
- Be sure a **full backup** occurs prior to test

The **goal** of BCDR testing is to ensure the **BCP process is:**

- **Accurate**
- **Relevant**
- **Viable** under adverse conditions

Plan Disaster Recovery and Business Continuity

Creating, Implementing, and Testing a Plan

Failover: Options to switch to BCDR systems
- **Cluster managers**
- **Load balancers**
- **DNS changes**
- Ensure these are not a **single point of failure**
- **Invoking BCDR actions** could be the responsibility of the client or the cloud provider, depending on the **contract**

Return to Normal
- **Failback** must be considered and tested
- If not tested, a failback can become a **serious outage**
- The BCDR site may become the **new primary site**
- **Premature failback** can cause serious problems
  - Must **ensure** the primary site is ready for failback

Creating a BCDR Plan
- **Define a scope**
  - **Roles** (who will do what)
  - **Risk** assessment
  - **Policies** (determine what constitutes a BCDR event)
  - **Awareness** for everyone involved
  - **Training** for everyone involved
- **Requirements**
  - Identify **business-critical services**
  - What **data** is involved
  - Any **service agreements** involved
  - List of **risks,** including failure of CSPs
  - Determine **RTO/RPO objectives**
  - Any **legal** or **regulatory compliance** involved

Creating, Implementing, and Testing a Plan

Creating a BCDR Plan (Cont.)

- **Analysis**
  - Translate requirements into a **design**
  - **Scope**, requirements, budget, performance objectives
  - Identify **mitigating controls** to be implemented
  - Consider **decoupling systems** to make BCDR more successful (ex: applications and databases)
  - **Ensure** CSPs and vendors can meet requirements
  - Identify **resource** requirements (storage, bandwidth, etc.)
- **Risk Assessment**
  - Evaluate **CSP's ability** 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 a second license)

Creating, Implementing, and Testing a Plan

Creating a BCDR Plan (Cont.)

- **Plan design:**
  - Establish and validate **architected solution**
  - Include **procedures and workflows**
  - Define **owner(s)**
    - Technical
    - Declaring BCDR event
    - Communications to customers
    - Internal communications
    - Decision makers
  - Describe **how BCDR plans will be tested**
    - Enterprise-wide testing plans should address **every** business-related service
    - Should be **fully tested annually** with semi-annual training (walkthroughs) 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**

Plan Disaster Recovery and Business Continuity

Creating, Implementing, and Testing a Plan

Testing Policy

- RTO/RPO must be **measured** to ensure attainability
- Testing **objectives** should start simple and expand to encompass the entire plan
  - Individual **services**
  - Internal and external dependencies
- Should include **test planning**
  - Scenarios
  - Measurable results (RTO/RPO)
- Should include a **test scope**
  - Master test scheduled that includes **all objectives**
  - Description of test objectives and methods
  - **Roles and responsibilities** for all participants
  - Define participants and **alternate participants**
  - Key **decision makers**
  - Testing **locations**
  - **Contact** information

Plan Disaster Recovery and Business Continuity

Creating, Implementing, and Testing a Plan

Greater frequency of testing provides greater confidence in BCDR activities.

Tabletop Exercise

- 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 the exercise
  - Each participant receives a **copy of the BCDR plan**

Walkthough 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 key personnel
- Demonstrates knowledge, teamwork, and **decision-making capabilities**
- Role-play and act out steps, identify issues, **solve problems**
- Involve **crisis management team** so they can practice as well

Cloud Development Basics

Cloud development typically involves:

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

In most cloud environments, **APIs** are used to access application functionality

- APIs use **tokens** for authentication

Most Common API Formats

- **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

REST vs. SOAP

- **REST supports many formats,** including JSON, XML, and YAML | **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**

Common Pitfalls

- **On-premises doesn't always transfer to cloud**
  - On-premises apps **were not developed** for the cloud environment
  - **Cloud may not support** the way an application works on premises
- **Not all apps are cloud-ready**
  - Can be **more challenging** to implement the same level of security in the cloud
- **Lack of training**
  - Cloud services may **work differently** than similar on-premises services
- **Lack of documentation and guidelines**
  - May be a lack of documentation by the CSP if **services are new**
  - **Follow** a software development lifecycle **(ISO/IEC 12207)**
- **Complexity of integration**
  - **CSP manages** part of the environment, and that can make integration **tricky** since the developers don't see the whole system
- **Other challenges:**
  - **Multitenancy** challenges
  - **Third-party** administrators (CSPs)

Common Vulnerabilities

Most common vulnerabilities are listed in the **OWASP Top 10**

- We'll cover this **in depth** in the **Applying SDLC** section

Business Requirements

Business requirements are part of the **first phase** of the **Secure Software Development Lifecycle (SDLC)**

- **Business needs** of the application
  - Accounting
  - Database
  - Customer relations (CRM)
- **Refrain** from identifying technologies at this point
  - Concentrate on the **needs of the business**

Phases and Methodologies

ISO/IEC 12207 is one example of an SDLC — there are many!

Common **SDLC phases** include:

- **Planning**
  - All **stakeholders** are involved
  - Business, security, and standard **requirements defined**
- **Defining**
  - **Document** all requirements and get approval
- **Design**
  - Design, identify impact on **architecture and hardware**
  - Threat **modeling and security** design
- **Development**
  - Coding starts
  - Longest phase
  - Code review and **static analysis** testing
- **Testing**
  - User **acceptance testing**
  - Testing of any integrations
- **Maintenance**
  - Fixing bugs
  - Patching vulnerabilities
- **Disposal**
  - Once the application is no longer required
  - Securely erase application data **(crypto-shredding)**

Phases and Methodologies (Cont.)

- Once an application goes into production, it enters the **secure operations phase**
  - **Versioning** is used to track changes
  - **Testing** of each version is performed
    - Dynamic analysis
    - Vulnerability scanning

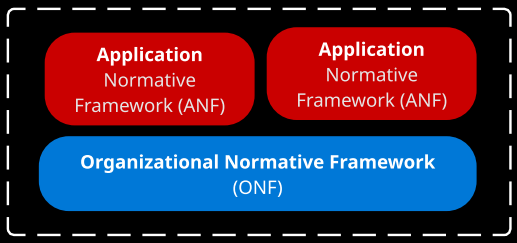
- **ISO 27034** is one of the most widely accepted set of standards and guidelines for **secure application development**

- ISO 27034 outlines the **Organizational 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:** Functional IT requirements and solutions to meet those 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

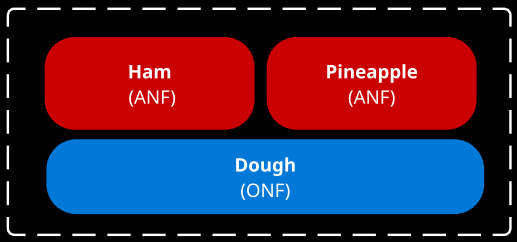
Phases and Methodologies (Cont.)

ISO 27034 also outlines the **Application Normative Framework (ANF)**

- Used in **conjunction** with the ONF
- Created specifically for a **single application**
- ONF to ANF is a **one-to-many relationship**



ONF + ANF



Pizza Making Process

Phases and Methodologies (Cont.)

Application Security Management Process (ASMP)

- Process of **managing and maintaining each ANF**
- Consists of five steps:
  1. **Specify** the application requirements and environment
  2. **Assess** application security risks
  3. **Create** and maintain the ANF
  4. **Provision** and operate the application
  5. **Audit** the security of the application

Common Vulnerabilities

OWASP Top 10

- **Injection:** Injection attacks occur 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 commands. SQL injection is a common example.
  - **Prevention:** Use input filtering to **verify** that 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, attackers can execute scripts in the victim's browser. Scripts can be posted in a forum, and visitors' browsers will execute the scripts.
  - **Prevention:** Validate inputs to ensure that data is expected and not malicious.

Common Vulnerabilities (Cont.)

OWASP Top 10 (Cont.)

- **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 to represent objects so the **real objects are never exposed.**
- **Security misconfiguration:** Mistakes in configuring the security settings of an application.
  - **Prevention:** Understand the application and its settings.
- **Sensitive data exposure:** Lack of security controls for 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 for the functions of a web application can allow attackers to forge requests and gain access to functions.
  - **Prevention:** Ensure all functions are accessed via an authorization module, and set a global rule to deny access by default.

Common Vulnerabilities (Cont.)

OWASP Top 10 (Cont.)

- **Cross-site request forgery (CSRF):** When an attacker uses an authenticated user's browser to send forged **HTTP** requests on behalf of the attacker.
  - **Prevention:** Use anti-forgery tokens to prevent CSRF attacks from being successful.

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

- **Invalid redirects and forwards:** Web applications sometimes use redirects to forward users to other websites. When these destinations are not validated, attackers can redirect users to malicious web sites.
  - **Prevention:** Avoid using redirects and forwards if possible. If you must use them, avoid involving user parameters when redirecting to the destination.

Common Vulnerabilities (Cont.)

- To identify and address these vulnerabilities, **application risk-management programs** should consist of three parts:
  1. **Framework core:** Activities and functions
     - Identify
     - Protect
     - Detect
     - Respond
     - Recover
  2. **Framework profile:** Align activities with business requirements, risk tolerance, and resources
  3. **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**

Cloud-Specific Risks

Some **cloud-specific risks** include:

- PaaS may not offer acceptable **encryption**, so it may need to built into applications
- PaaS may not offer granular security
- **Logging** may be difficult for SaaS applications
- Lack of **proper access controls**

The "Notorious Nine" Cloud Computing Threats

1. Data breaches
2. Data loss
3. Account hijacking
4. Insecure APIs
5. Denial of service (DoS)
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence (on behalf of the customer)
9. Shared technology use (multitenancy)

Cloud-Specific
Risks

Quality Assurance

Measure the following **variables** to ensure that quality standards are being met:

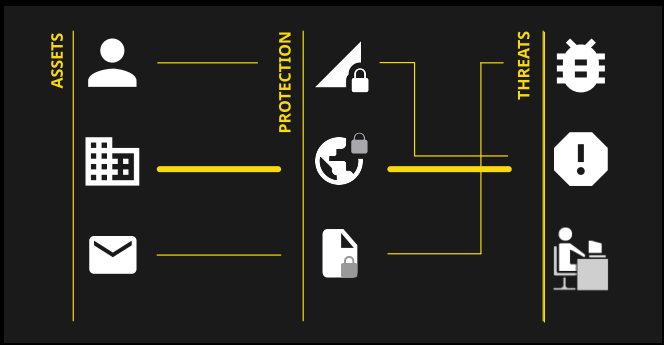
1. **Availability**
2. **Mean time between failures (MTBF)**
3. **Outage duration**
4. **Performance**
5. **Reliability**
6. **Capacity**
7. **Response time**

Quality
Standards

Threat Modeling

- **Threat modeling:** The process of identifying, communicating, and understanding threats and how to mitigate them in order to **protect valuable assets**
- The **STRIDE threat model** is a system for classifying known threats based on the kinds of exploits used or the motivation of the attacker. **STRIDE** describes the following six threats:
  1. **S**poofing
  2. **T**ampering
  3. **R**epudiation
  4. **I**nformation disclosure
  5. **D**enial of service
  6. **E**levation of privileges

Example Threat Model



Software Configuration Management and Versioning

Two popular tools for configuration management and versioning:

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

CHEF

puppet

The purpose of these tools is to **ensure** configurations are up to date and **consistent** based on the version of a policy or configuration.

Functional Testing

Functional testing is used to **verify that business requirements** have been met and the **application operates as expected** without errors.

Functional
Testing

Cloud Application Security

Software Assurance and Validation

Security Testing Methodologies

Two main types of security testing:

- **Static Application Security Testing (SAST):** Considered a **white-box** test — the test performs an analysis of the source code and binaries without executing the code.
  - SAST is used to **identify coding errors** that may indicate 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 — 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. **SAST is used early on** in development to detect coding problems, while **DAST** is used to identify vulnerabilities **while the application is running.**

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

Cloud Application Security

Software Assurance and Validation

Security Testing Methodologies (Cont.)

- **Vulnerability assessment:** Scanning an application with a vulnerability scanner or assessment tool such as **BURP** or **OWASP ZAP.**
  - Look for well-known vulnerabilities
  - Uses **signatures** to identify vulnerabilities
    - No signature = no identification of vulnerability
- **Penetration test:** Process of collecting information about a system and using it to **actively exploit** any vulnerabilities and gain access to the system or its data.
  - Considered a **black-box** test
- 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:** Manually reviewing code and looking for vulnerabilities. (static testing)

Security Testing Methodologies (Cont.)

OWASP has created a testing guide that includes **nine testing categories:**

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

Approved APIs and Third-Party Software

Application programming interfaces (APIs) expose the 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 like any other component used in the creation and use of applications.

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

- 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 Dependency-Check

API

Approved APIs and Third-Party Software (Cont.)

- 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 that we use.

- **Open-source software** is considered relatively secure because the source code is **open and available** for anyone to review.
  - This means the code is subject to a great deal of **scrutiny** for best practices and functionality.
  - Third-party software is **often created in a closed environment** with minimal review and testing, due to time and budget constraints.

Supplemental Security Components

Supplemental security components add additional layers to a **defense-in-depth strategy.**

Supplemental Security Components

- Web application firewall **(WAF)**
  - **Layer 7** firewall that can understand HTTP traffic calls (GET, POST, etc.)
  - Effective for **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**
  - Acts as a **go-between** for access to an API
  - Uses access rules to **prevent access to APIs**
  - Can implement other controls such as **DLP, antivirus, and anti-malware services**
- Firewalls
  - Provide filtering capabilities
- **API gateway**
  - **Filters API traffic** before it is processed
  - Can provide **access control, rate limiting, logging, metrics, and security filtering**

Cryptography

When accessing data in the cloud, we access the data across trusted and **untrusted networks.** It is important to **protect the data,** and one way to do that is to **use encryption.**

Protecting Data in Motion

- **Transport Layer Security (TLS):** TLS ensures data privacy and integrity between applications.
  - Uses **x.509** certificate to authenticate initial connection
  - Transfers **symmetric encryption key** to be used
- **Secure Socket Layer (SSL):** The standard technology for creating an encrypted connection between a browser and a web server. All data passed through the connection is kept private and maintains its integrity.
- **IPSec virtual private network (VPN):** Encrypts data between two endpoints. These endpoints can be firewalls, VPN concentrator devices, or 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.

Sandboxing and Application Virtualization

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.**

Application Virtualization

- Used to test applications while **protecting the underlying OS** and other applications on the system
- A form of **sandboxing an individual application** on a host
- Commercial examples:
  - **Wine**
  - **Microsoft App-V**
  - **XenApp**

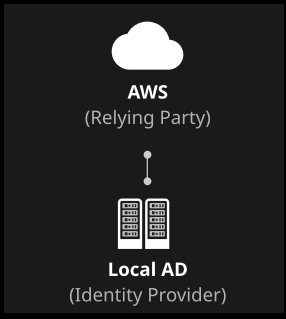
Federated Identity

Federated identity allows for **trusted authentication across organizations.**

Identity Federation Standards

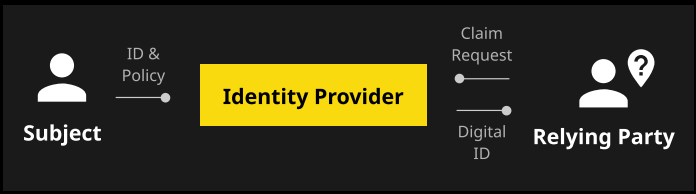
- **Security Assertion Markup Language (SAML):** The most common federation standard
  - SAML is XML-based
- **WS-Federation:** Defines mechanisms that allow different security realms to federate between each other
- **OpenID Connect:** Lets developers authenticate their users across websites and apps 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 education websites and apps

A federation consists of an **identity provider** and a **relying party.**



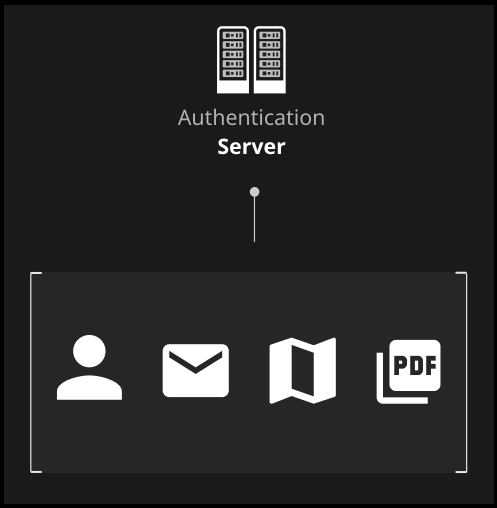
Identity Providers

Identity providers perform authentication services and pass required information to **relying parties** as needed, supplying the required authorization to access resources.



Single Sign-On (SSO)

- Single sign-on (SSO) allows a user to **authenticate once** and then access multiple resources instead of having to authenticate with each individual resource.
- With SSO, a user logs in to an **authentication server**. Then each resource the user attempts to access checks with the authentication server to verify that the user has already successfully logged in.



- SSO makes the **user experience more pleasant**.

Multi-Factor Authentication (MFA)

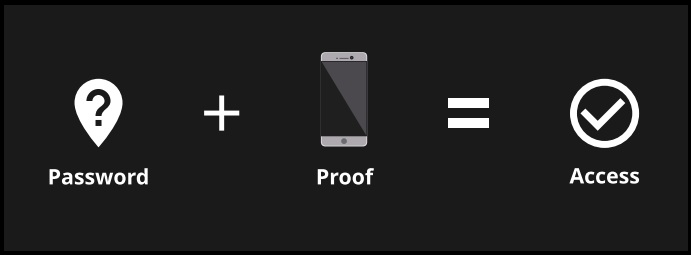
Multi-factor authentication: Using **multiple factors** to authenticate. These factors are based on:

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

One-time passwords fall under MFA and are highly encouraged for use with first-time logins (you must change your password).

Step-up authentication is used during **high-risk transactions** or when violations have occurred in a transaction.

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



Cloud Access Security Broker (CASB)

- **CASB:** A **trusted third-party identity provider** that manages authentication between cloud service users and cloud applications.
- 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:** 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 a **CASB.**

What is a Cloud Access Security Broker (CASB)?

Hardware Security

Securing Servers

- Follow OS vendor **recommendations** for secure deployment
- Remove all **unnecessary services**
- Install all **patches**
- Lock down the host
  - **Restrict** root/admin access
  - Use only secure communications (SSH)
  - Use host-based **firewalls**
  - Use role-based access control **(RBAC)** permissions
- Secure management practices
  - Ongoing patching and maintenance
  - Periodic **vulnerability** scanning
  - **Periodic** penetration testing

Virtualization Management Tools

It is **extremely important** to properly configure virtualization management tools.
- If compromised, an attacker could gain **full access** to the virtual environment.

All management should take place on an **isolated network.**

The **virtualization vendor** will determine which tools can be used.
- Plan to **maintain and update** the tools.
- Plan for maintenance windows and **VM migrations** between hosts to allow for updates and reboots.
- Perform **vulnerability testing** on the tools.
- 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 the tools.
- **Auditing and monitoring:** Track and validate use of the tools.
- **Maintenance:** Update the tools as necessary and follow vendor recommendations.

Virtualization Management Tools (Cont.)

- Secure configuration **templates should be used** to configure virtualization hardware
  - Templates should be saved in a **secure manner**
  - Update templates via formal **change management** process
- Virtual hardware should be configured to **log sufficient data**
- **Guest OS Virtualization Tools**
  - Provide **additional functionality**
  - Must be maintained and updated
  - **Vulnerability scans** should be conducted

Back
Next
Back to Main

Access Control for Local and Remote Access

- Physical access should be **limited.**
  - Individuals who manage physical hardware should not have other types of administrative access **(separation of duties).**

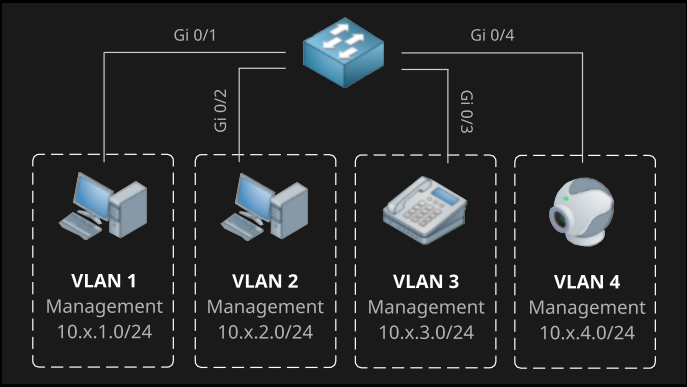
- **Remote access** to physical hosts should be done via **secure KVM switch (keyboard, video, mouse)**
  - Access to the KVM should be **logged and routine audits** conducted.
  - KVMs provide secure access and **prevent data loss.**
  - **MFA** should be considered for KVM access.

- **Requirements for Secure KVMs**
  - **Isolated data channels:** Each channel connects to only one host so that no data can be transferred between connected computers through the KVM
  - **Tamper warning labels:** Located on each side of the KVM — indicate tampering
  - **Housing intrusion detection:** Renders the KVM inoperable if the housing has been opened
  - **Fixed firmware:** Firmware cannot be reprogrammed — prevents tampering
  - **Tamper-proof circuit boards**
  - **Safe buffer design:** No memory buffer to retain data
  - **Selective USB access:** Only recognize human interface USB devices, such as keyboards and mice, to prevent data transfer to USB mass storage devices
  - **Push-button control:** Require physical access to the KVM to switch between computers

Secure Network Configuration

Isolating Networks with VLANs

- All **infrastructure management** should occur on an isolated network (VLAN).
- VLANs are used to **created isolated networks** for customers in a multitenancy environment.
- VLANs work by **tagging data with a VLAN ID,** which 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 on switches

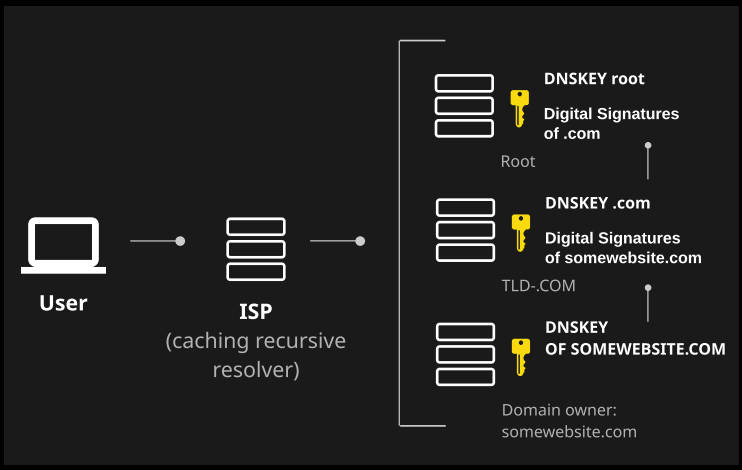


Secure Network Configuration (Cont.)

DNSSEC

- Adds security to DNS by allowing DNS responses to be **validated**
- DNSSEC uses a process called **zone signing,** which uses digital certificates to sign DNS records
- **Prevents pharming attacks** (fake website credential harvesting)

DNSSEC



Secure Network Configuration (Cont.)

Threats to DNS

- **Footprinting:** An attacker attempts to gather all DNS records for a domain via **zone transfer** in order to map out the target environment
- **Denial of service (DoS):** Attackers flood DNS servers to prevent them from responding to legitimate DNS requests
- **Redirection:** An attacker redirects queries to a server that is under the attacker's control
- **Spoofing:** An attacker provides incorrect DNS information for a domain to a DNS server, which then gives out that incorrect information (also known as **DNS poisoning**)

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 data encryption
- Operates in one of **two modes:**
  - **Tunnel** — Encrypts the entire original packet and provides a new header (supports **NAT traversal**)
  - **Transport** — Only encrypts part of the original packet

OS Hardening with Baselines

- **Baselines** are an agreed-upon set of attributes for a product.
- **Configuration management** tools such as Puppet and Chef can ensure operating systems are hardened according to a given 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 the **change management process**

Stand-Alone Hosts

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

Disadvantages of Stand-Alone Hosts
- **Lack** of elasticity
- Lack of clustering benefits
- **Higher** costs

Benefits of Stand-Alone Hosts
- **Isolation**
- Dedicated host
- **More secure** (not a multitenant host)

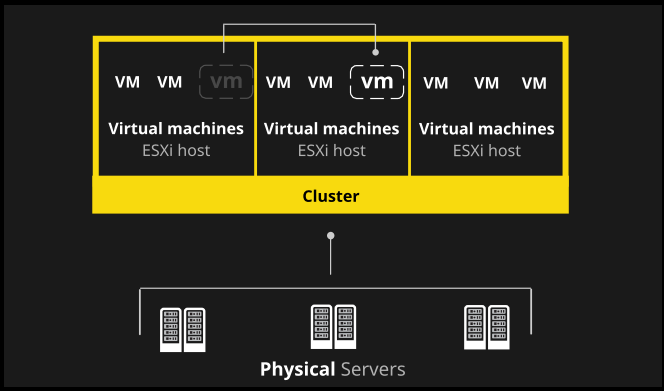
Driving Factors for Use of Stand-Alone Hosts
- **Regulatory** issues
- Data **classification**
- **Contractual** requirements
- **Security policies**

Cloud Security Operations

Operate Infrastructure

Availability of Clustered Hosts

- A **host cluster** is a group of centrally managed servers that allows for failover and VM migration between hosts.
- **Resources are pooled** within a cluster. Prevent resource starvation with:
  - **Reservation limits:** Reserving a minimum amount of resources
  - **Shares:** Used to guarantee an amount of resources during times of resource constriction



- Clusters provide **high availability (HA)**.
  - If a host goes down, the **VMs migrate to another host**.
- Clusters use **distributed resource scheduling (DRS)**.
  - A resource manager uses **rules to balance the workload**.
  - Affinity rules can be used to **keep VMs on the same host**.
  - **Anti-affinity rules** keep VMs on separate hosts.

Availability of Guest Operating Systems

- Availability is **increased** with the use of:
  - **Secure** practices
  - **Clustering**
  - **High-availability** solutions

- Availability is **measured** in a percentage known 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

Access Control for Remote Access

Key Features of a Remote Access Solution

- Accountability of remote access with an **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 that the user is connecting to — virtual desktop infrastructure (VDI)

Remote
Access

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** (sing up)
  - 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 (**roll back plan**)

Patch Management Cont.

- Patch management **challenges:**
  - Lack of **standardization** of patches
  - Collaboration between **multiple system owners**
  - Many moving parts (**complexity**)
  - Patches must be **tested** before deployment
  - VM's in a **suspended state** are not patched
  - Multiple **timezones** (applying patches at same local time)

- In some cases, organizations may give **blanket approval** for applying patches which address iminent risks, allowing these patches to **bypass standard change management process**. Change management will take place after the fact.

Performance, Capacity, and Hardware Monitoring

Monitoring performance and capacity is **critical**.
- Changes in performance can indicate **failing hardware**.
- Unmonitored capacity could allow for total consumption of resources, which can lead to **resource starvation** and a **serious impact on performance**.

Items to Monitor on Host Hardware
- Excessive **dropped packets** on network interfaces
- Disk **capacity and IO**
- **Memory** utilization
- **CPU** utilization

In a **shared environment**, monitoring is crucial for maintaining an acceptable level of performance.

In a virtualized environment, everything still runs on **underlying hardware** that must be monitored.
- **Environmental** temperatures
- Temperature within **hardware**
- **Fan speeds**
- Failed drives or **drive errors**
- Hardware components **(CPU, memory, cards)**
- **Network devices** (not just servers)

Backup and Restore Functions

- **Host configuration data** should be included in backup plans.
- **Routine tests** should be conducted to test the restorability of backup data.
  - **Individual file** recovery
  - **Entire VM** image recovery
  - **Increases the likelihood** of a successful BCDR failover
- 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:** The ability to monitor data and how it's being accessed.
  - This is why testing is so **critical**.

Network Security Controls and Management Plane

Review of Network Security Controls

- Vulnerability assessments
- Network **security groups** (access lists)
- VLANs
- **Access control** (IAM)
- Secure protocols (SSH, TLS, SSL, IPSec)
- IDS/IPS
- Firewalls
- **Honeypots**
- **Zoning** of storage traffic (LUN IDs)
- Vendor-specific security products
  - VMware vCloud Networking and Security
  - Security or NSX products
- Keep public data and private data on **separate virtual switches**

Network Security Controls and 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

The management plane is **high-risk** and must be protected with:

- **Access control**
- **Logging**
- **Isolated network**

Other actions that can take place in the management plane:

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

Change Management

ISO 9001 — Quality and change management

Change Management Objectives

- **Respond** to changing business requirements while minimizing incidents and disruption
- Ensure changes are **documented** in a change management system
- Ensure changes are prioritized, planned, and tested
- Reduce overall **business risk**

Cloud Security Operations

Operational Controls and Standards

Continuity Management

- **ISO 22301** — Business continuity
  - Specifies requirements for **planning** the necessary procedures for restoring a business to an 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 identifies the systems and services that are critical to the business.

- **Continuity Management Plan**
  - Defines **events** that will put the plan in motion
  - Defines roles and responsibilities
  - Defines continuity and recovery **procedures**
  - Specifies which notifications are required to be sent
  - Specifies requirements for the capabilities and capacity of backup systems

- Business continuity plans should be **tested regularly**.

Back

Next

Back to Main

Information Security Management

ISO 27001 — Information security management

Organizations should have a documented **information security management plan** that covers:

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

ISO
27001

Incident Management

ISO 27035 — Security incident management

The **goal** of incident management is to:

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

Cloud Security Operations

Operational Controls and Standards

Problem and Deployment Management

- **ISO 20000** — Problem management & release and deployment management
- The **goal** of problem management is to minimize the 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:** A temporary way of overcoming a problem or known error
- A **system** should be in place to track problems and document root causes and workarounds.
- **Release and Deployment Management**: Includes planning, scheduling, and controlling the movement of releases to test and live environments
- The **goal** is to protect the integrity of the live environment.
- **Objectives of Release and Deployment Management**
  - Define **deployment plans**
  - Create and test release packages
  - Record and track packages in the **Definitive Media Library (DML)**
  - Ensure **functionality and requirements** are met
  - Manage risks
  - Ensure **knowledge transfer**

Back Next

Back to Main

Cloud Security Operations

Operational Controls and Standards

Configuration and Service Level Management

- **ISO 10007** — Quality management (includes configuration management)

- The **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

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

- **Common Agreements**
  - **Service-level agreement (SLA):** Between the customer and the provider
  - **Operational-level agreement (OLA):** SLA between business units within an organization
  - **Underpinning contract (UC):** External contract between the organization and a vendor

- The organization's **legal department** should be included in contract creation.

Back

Next

Back to Main

Cloud Security Operations

Operational Controls and Standards

Availability and Capacity 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
- **High availability (HA)** and failover solutions help maintain availability

ISO 20000 — Capacity management

- Ensure infrastructure is **adequately provisioned** to meet SLAs in a cost-effective manner
- Monitor capacity to **prevent performance impact**

Forensic Data Collection Methodologies

Forensic Data Collection Process

1. **Collection of evidence** — Identification, labeling, recording, preservation of data integrity
2. **Examination** — Processing evidence, extracting data while preserving data integrity
3. **Analysis** — Deriving useful information from evidence
4. **Reporting** — Reporting on findings, including tools and procedures used, recommendations, and alternate explanations

Data Collection

1. Develop a **plan** that specifies which sources are to be collected and in what order.
   - **Value** — Relative likely value of data sources (from past experiences)
   - **Volatility** — Likelihood that data will be lost on a system when it is 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 between effort and the likelihood that data will be valuable
   - **Chain of custody** should be implemented

Forensic Data Collection Methodologies (Cont.)

Data Collection (Cont.)

2. **Acquire the data.**
   - Use **forensic tools** to gather data (write blockers)
   - Create **duplicates of data** to work with
   - **Secure the original**, non-volatile data (create a hash if possible)

3. **Verify the integrity of the data.**
   - Use the **hashed value** of the original data to verify that the working copy has **not been altered**

Data Examination

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

Analysis

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

Forensic Data Collection Methodologies (Cont.)

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 requires the collection of additional information.

Challenges with Collecting Evidence

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

Forensic Data Collection Methodologies (Cont.)

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

- Packet capture 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

Network Forensics Use Cases

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

Evidence Management

- Be sure not to collect evidence **outside the scope** of the event.
- **Chain of custody** is used to track and manage evidence, from identification to disposal.
  - At **each stage**, document who is involved, record the date and time, and sign the chain of custody.
  - More information is better.
  - Record when evidence is **moved**.
  - Record when **analysis** takes place and what type of analysis.
  - **NEVER** work from the original data; always work from a copy.
- There are **many standards governing** 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 analysis of digital evidence
  - **ISO/IEC 27050-1:2016** — Guide to e-Discovery

Managing Communications

Vendor and Partner Communications

- **Identify and document** all partners, ensuring the relationship is understood.
  - The **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**.

Customer Communications

- 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.

Managing Communications (Cont.)

Regulators

- **Early communication** is key when developing a cloud environment (surprises cost time and money).
- Regulatory **requirements vary greatly** based on:
  - Geography (**jurisdiction**)
  - Business type (e.g., medical, financial)
  - Services offered (e.g., processing credit cards or personal data)
  - Data type (classification, sensitivity)
- It is **imperative** that a organization understand all regulatory compliance needs **prior to planning** a cloud environment to ensure they can all be met.

Security Operations Centers

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 behavior and signs of compromise
- **Analyze** system logs
- Protect the organization from attacks
- Perform **vulnerability scans**
- Monitor **internet traffic** and other traffic flows
- Handle asset discovery and management
- Assist with incident response

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

Monitoring Security Controls

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

- **Firewalls**
- IDS/IPS
- Honeypots
- **SIEMs**
- **Vulnerability scans**
- Network security groups
- **System logs**
- Endpoint security solutions

These systems are hardware- and software-based, and they ***will* fail at some point.**

Security
Controls

Log Capture and Analysis

- Various tools are available to collect and analyze log data from **event sources**, including:
  - **Host servers**
  - **Guest operating systems**
  - **Network devices**
- **Centralized and offsite** storage of log data can prevent tampering.
- **Security Information and Events Management (SIEM)**
  - Used to centrally collect and analyze logs
  - Can create specific event **alerts 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**, and a SIEM or Syslog server will keep a safe copy of the system logs for analysis.

Cloud Security Operations

Manage Security Operations

Incident Management

Incident Management
- Activities of an organization to identify, analyze, and correct hazards to prevent future incidents
- An **incident response team (IRT)** usually handles these activities

Incident Response Objectives
- Ensure **standardized** incident management methods are used
- Ensure visibility and **communication** of incidents to support staff
- Align incident management activities with **business goals**

Incident Management Plan
- **Definitions** of incidents
- Roles and responsibilities of CSP and customer
- Incident management **process to follow**
- Media coordination
- Legal or regulatory **notification requirements**

Incident Prioritization
- **Impact** — Effect on the business
- **Urgency** — Can resolution be delayed?
- **Priority** = Impact (times "*") Urgency

Conflicting International Legislation

Cloud computing introduces many **legal challenges** for the security professional.

- **Conflicting** legal requirements
- **Lack** of clarity

International Laws

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

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

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

Conflicting International Legislation (Cont.)

- **The doctrine of the proper law:** When a conflict between 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 that protect the safety and well-being of the public.
- **Tort law:** Rules and regulations designed to seek relief for personal suffering as a result of wrongful acts.
  - **Compensate** victims
  - **Shift the cost** of injuries to the offender
  - **Discourage** careless and risky behavior
- **Restatement (second) conflict of laws:** Laws **made by judges** — not legislation — 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.

Legal
Risk

Legal Risks Specific to Cloud Computing

One risk is the potential **loss of control over 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 that the CSP is to inform you of any such events
- Ensure the contract states that **you are to be in charge** of making decisions about your data and how it is handled in response to a subpoena or other legal action

Legal Frameworks and Guidelines

Organization for Economic Cooperation and Development (OECD) Privacy and Security Guidelines

- The OECD published **guidelines governing** the privacy and protection of personal data flowing across borders; focused on the need for global privacy protection.

Asia-Pacific Economic Cooperation (APEC) Privacy Framework

- Consists of 9 principles and 21 member countries; provides a regional standard to **address privacy as an international issue** and cross-border data flows.

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**.

- **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 illegal to process data related to racial or ethnic origin, political preference, religious beliefs, trade union affiliation, or data concerning health or sexual status.
- Data subjects' right to access data:
  - **Confirmation to the data subject** if data about that subject is being processed.

Legal Frameworks and Guidelines (Cont.)

General Data Protection Regulation (GDPR): Designed to protect all EU citizens from privacy and data breaches. Differs from the EU Data Protection Directive in the following ways:

- Applies to all companies **processing data of EU citizens**, regardless of 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 — must be in **intelligible and easily accessible format**
- **Notification of a breach** 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.
- GDPR is the primary privacy law throughout **all EU member states and *supersedes local privacy laws***.

ePrivacy Directive: Created by the European parliament to protect the privacy of data that is processed in the electronic communications sector.

Legal Frameworks and Guidelines (Cont.)

U.S. 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)** in place.
- **Children's Online Privacy Protection Act (COPPA):** Created to protect the privacy of children under 13 on the internet.
- **Sarbanes-Oxley Act (SOX):** Holds company executives accountable for data accuracy in an effort to prevent fraud and protect shareholders and employees.

Standards

- **ISO & NIST**
- **Payment Card Industry Data Security Standard (PCI-DSS):** Designed to protect cardholder information.

Silver Platter Doctrine: Former doctrine of criminal law that stated a federal court could introduce illegally or improperly seized evidence, as long as federal officers had played no role in obtaining it.

- **Ex:** If an employer discovered that one of their employees was stealing and selling sensitive company data, they could collect the evidence and give it to law enforcement. That evidence could legally be used in court because law enforcement was not involved in collecting it.

e-Discovery

e-Discovery (ISO 27050): 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 (requires cooperation of remote CSPs in **different jurisdictions**)

Conducting e-Discovery Investigations in the Cloud

- **SaaS-based e-discovery:** Some packages may be available for discovering, collecting, and preserving data in the cloud
- **Hosted e-discovery provider:** You can hire a hosted service provider to perform e-discovery for you
- **Third-party e-discovery**: Outsourcing to an organization that specializes in cloud-based e-discovery

Forensic Requirements

- **Cloud forensics:** The practice of reconstructing 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 — e-Discovery:** Works to globally standardize approaches to cloud forensics.
- Ensure that **individuals collecting forensic data are trained and certified in the tools they use**, as this will lend credibility to their findings.

Contractual vs. 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 any data they upload to the CSP.
- **Personally identifiable information (PII):** Any data that can be used to identify, contact, or locate a living individual. Includes a person's social security number, driver's license number, address, phone number, date/place of birth, mother's maiden name, and biometric records.
- **Two main types of PII** related to the cloud:
  - **Contractual PII:** An organization processes, transmits, or stores PII as part of its business or services. Contractually, this data must be protected by the business providing the service.
  - **Regulated PII:** PII must be protected due to the legal and statutory requirements of regulations such as HIPAA and GLBA. Regulatory protection shields individuals from risk.

  - **Both must protect PII**, but one is for contractual reasons while the other is for regulatory reasons.
  - Another **difference** is that with regulated PII, breach reporting is mandatory.
  - **NIST 800-122** is a useful resource for ensuring that the requirements for contractual and regulated PII are being met.

Contractual vs. Regulated Private Data (Cont.)

Contractual Components

- **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:** Ensure that the data deletion process meets organizational policies
- **Data security controls:** Security controls should be implemented at the same level across the processing organization and any subcontractors involved in the process
- **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 the data processing as well as any subcontractors involved in the process

Country-Specific Legislation Related to Private Data

European Union

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

- To **transmit EAA citizens' personal data outside their country**, companies must abide by Directive 95/46 EC in the EU or the Safe Harbor/Privacy Shield program in the US.

Directive 95/46 EC: Specifies provisions for the protection of individuals with respect 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 the rights of individuals to protect their personal data. GDPR introduces some new changes such as:

- The 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** to a person who declines to participate in data collection

Country-Specific Legislation Related to Private Data

According to GDPR, an **entity outside of the EU** can gather/process personal data belonging to EU citizens if the entity:

- Is **located in a country** with a national law that complies with EU laws
- Creates **binding contractual wording** that complies with EU laws
  - Each country in the EU for which data is processed must **approve** the wording of the contract
- Joins 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 applicable US laws and regulations apply to data after it leaves the US, and the US-regulated **entities that send data abroad remain liable for:**

- Data **exported** outside the US
- The processing of data by **subcontractors outside the US**
- Subcontractors abroad using the same level of **protection for regulated data**

Country-Specific Legislation Related to Private Data

- **Safe Harbor Program:** Developed by the US and EU to address concerns that the US does not have a regulatory framework that provides adequate protection for personal data transferred from the European Economic Area (EAA).
- **Privacy Shield Framework:** As of July 12, 2016, the EU reversed its decision on the legal adequacy of the US Safe Harbor program. The US has now implemented the Privacy Shield Framework, 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 (FTC)**.
- **Stored Communications Act (SCA):** Provides privacy protection for electronic communication and computing services from unauthorized access or interception.
  - **Very outdated** and in need of updating
- **Cross-Border Data Transfers:** Canadian regulations covering the processing of Canadian citizens' data outside of Canada.

Jurisdictional Differences

- **Many countries**, including Switzerland, Argentina, Australia, and New Zealand, follow similar data privacy rules as the EU.
- **CCSPs should always engage with legal professionals** about local and international laws prior to engaging in cloud services.

Jurisdictional
Differences

Standard Privacy Requirements

- **ISO/IEC 27018:** Addresses privacy in cloud computing and consists of 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 have access to PII.
  - **Communication:** CSPs must keep record of all incidents and their responses to them, as well as 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 that are very similar to the OECD and GDPR principles.
- **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.

Audit Controls and Requirements

- 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.
  - Audit the **greatest risks**
- **External audits** focus on the controls over financial risk.
  - Areas that support the financial health of the organization
  - Don't necessarily focus on cloud risks
- 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 tech-savvy** is the CSP that's providing you data?
  - We can only **do our best** and attest to what data is provided to us.

Assurance Challenges of Virtualization and the Cloud

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

As CCSPs, we're concerned with ensuring the 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 you plan the assessment and associated testing
- Verify that systems are following security **best practices**
- Ensure that **configurations** are done according to organizational policy

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

Types of Audit Reports

- **American Institute of CPAs (AICPA) Service Organizational Control (SOC) 1, 2, and 3 Reports**
  - **SOC 1** — Validating **financial** statements and risks
  - **SOC 2** — Validating the effectiveness of controls in a **technically detailed** format
    - **Type 1:** Reporting the effectiveness of controls at a specific **point in time**
    - **Type 2:** Reporting the effectiveness of controls **over a period of time** (generally 6 months)
  - **SOC 3** — Validating the effectiveness of controls in a **generalized** format
- **International Standard on Assurance Engagements (ISAE):** The international equivalent to a SOC 1 report
- **Agreed-Upon Procedures (AUP):** Based on the Statement on Standards for Attestation Engagement (SSAE), in an AUP an auditor is engaged to report on the findings of procedures performed by the audited party. **The auditor provides no opinion, only states identified facts** and the third party forms their own conclusion based on the report.
- The **Cloud Security Alliance (CSA)** has created the **Security, Trust and Assurance Registry (STAR)** program.
- **EuroCloud Star Audit (ESCA) program:** European CSP certification program

Restrictions of Audit Scope Statements

Audit scope statement: Provides the necessary information 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 to:

- **Limit the operational impact** of audit activities
- **Lower the risk to production** environments posed by audit activities
  - **Ex:** The auditor cannot require a fully functional disaster recovery test.
  - **Ex:** The auditor cannot pull the fire alarm unannounced to verify functionality.

Cloud service audits are primarily based on:

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

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

Gap Analysis

Gap analysis: Used to identify gaps between an organization's environment and the frameworks or standards that the organization is attempting to comply with.

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

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

A gap analysis is **often performed internally** by someone outside the department being audited.

Audit Planning

Four Phases of Audit Planning

1. Define the 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. Define the audit scope.
- **Define** the 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

3. Conduct the audit.
- Adequate **staff**
- Adequate **tools**
- **Schedule**
- Take **previous audits** into account

4. Refine the audit process & review lessons learned.
- Ensure the **scope is still relevant** after review
- Factor in any **provider changes** since the last audit
- Identify opportunities for **report improvements**
- Ensure scope criteria and scope are **still accurate** after review

ISMS (Internal Security Management System)

ISO 27001: A standard that defines information security management systems (ISMS) and is used to **measure a comprehensive security program.**

Internal audits should be part of every ISMS program.
- **Reduce risks** related to the availability, integrity, and confidentiality of data
- Improve **stakeholder confidence**

ISO 27001 covers security control systems within an ISMS.
- Security controls are mapped to requirements identified through a formal risk assessment

ISO 27001 covers several domains, including:
- A.5 — Security policy management
- A.8 — Organizational asset management
- A.10 — Cryptography policy
- A.11 — Physical security policy
- A.13 — Network security management
- A.18 — Security compliance management

An **ISMS helps standardize and measure** security across an organization and to the cloud.

Policies

Organizational policies affect the organization as a whole.
- **Ex:** *The organization will follow accepted standards to protect client data.*

Functional policies are key to implementing an effective data security strategy.
- **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.
- Password policy
- **Remote access** policy
- Encryption policy
- **Third-party access** policy
- Segregation of duties policy
- **Data backup** policy

Policy

Involvement of Relevant Stakeholders

It's **extremely important** to involve relevant stakeholders from the beginning of a cloud computing discussion.

- Help provide an **overarching view** of organizational processes
- Ensure the approach to cloud **fits** and doesn't become a one-off

Stakeholder Challenges

- Defining an enterprise architecture
  - Consider **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**
  - Training
  - New tasks
  - New responsibilities
- **Extending risk management** to the cloud
  - New way of thinking about things

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):** Specifies protection for personal health information used in the healthcare services industry.
- **Payment Card Industry (PCI):** Regulates the handling and storage of credit card data.
  - Over **200 controls** in the standard
  - **4 merchant tiers** within the PCI DSS standard
    - Based on the number of transactions a merchant processes
    - Different merchant tiers determine the number of audits each must conduct

HIPAA NERC CIP PCI

Impact of the Distributed Information Technology (IT) Model

Clear communication is more challenging.

- Remote workers require a **re-thinking** of internal communication processes.
- Processes must be put in place to address requests in a **structured** way.
- Teams may span multiple geographical locations and **time zones**, and work schedules may need to be adjusted.
- Employees may be in several different **legal jurisdictions**.

Gathering information from resources is different.

- Information used to come from a team of employees; now it comes from members of that group and from a CSP.

It may be beneficial to hire a **third-party consultant** to assist with the transition to a distributed IT model.

Distributed
Information

Back
Next

Back to Main

Assessing a Provider's Risk Management Framework

Key Steps

- **Review** security controls that are in place
- Identify the **methodologies or frameworks used** by the provider
- Review the **provider's policies**
  - May be posted on their website

Helpful Tips

- Look for CSPs who participate in the **CSA STAR program**

Cloud Security Alliance

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 meet its goals

Data Owners, Controllers, Custodians, and Processors

- **Data subject:** The person who is the focus of personal data
- **Data owner:** Holds the legal rights to and has complete control over data and can determine the distribution of said data
- **Data controller:** The person or organization that determines the manner in which data is processed and for what purposes
- **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)

Regulatory Transparency Requirements

- Many regulations require **breach notifications** to be sent to individuals whose information has been compromised.
  - **GDPR:** Within 72 hours
  - **HIPAA:** No later than 60 days
  - **PCI:** No requirement
  - **Most states** within the US have laws regarding breach notifications
- **Many other regulations** require organizations to be transparent with individuals whose personal data they maintain.
  - **GLBA**
  - **SOX**
  - **GDPR**

Breach
Notification

Risk Treatment

Four Ways to Handle Risk

- **Avoidance:** Simply avoid the risk (e.g., deciding not to use a specific service because it introduces more than an acceptable amount of risk).
- **Acceptance:** Accept the 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 mitigate risks.

3 Main Types of Security Controls

- **Physical:** Limiting physical access using 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

Risk Frameworks

ISO 31000 — Guidance standard **not intended for certification purposes**

- **Does not address** specific or legal requirements related to risk assessment or management
- Provides a **structured and measurable risk management** approach to assist with identifying cloud-related risks
- Lists 11 key principles as a set of guidelines
- **Focuses on** risk identification, analysis, and evaluation through risk treatment

ENISA — ***Cloud Computing: Benefits, Risks, and Recommendations for Information Security***

- Can be used as an effective foundation for risk management
- Identifies **35 types of risks to consider** and the top 8 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 used by the **US government and related agencies**

Back
Next
Back to Main

Metrics for Risk Management

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

- **Critical**
- High
- **Moderate**
- Low
- Minimal

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

Risk Metrics

- Number of **high-risk assets**
- Number of identified risks
- Number of recurring risks
- **Risk severity**
- Median time to discover risk
- **Median time** to remediate risk

Assessment of Risk Environment

What type of risk does the organization face?

Depends on several things:

- **Service:** What type of cloud services are being used and the what are the associated risks?
- **Vendor:** What is the vendor's reputation? What standards do they comply with?
- **Infrastructure:** Does the infrastructure follow best practices and meet compliance?

ISO 27002: Code of practice for information security controls

Information security controls are how we **address risk**.

Legal, Risk & Compliance

Outsourcing and Cloud Contracts

Business Requirements

Identify the business needs and requirements for moving to the cloud.

Define a scope of what will move to the cloud, including:

- **Services included** in the move
- Regulatory or legal **compliance required**
- **Risks associated** with the service and/or move to the cloud

Contract Types

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

Vendor Management

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

- Is the vendor **mature?**
- Is the vendor **financially stable?**
- Is the vendor **outsourcing services?**
- Is the vendor **compliant with industry standards?**
- Can the vendor meet **your regulatory compliance needs?**

Industry Standards to Consider

- **Common Criteria (CC):** An international set of guidelines and specifications (ISO/IEC 15408) developed for evaluating information security products to **ensure that they do what they say they do.**
- **CSA STAR:** Created to establish transparency and assurance for cloud-based environments. Allows customers to assess the security of CSPs by asking the CSPs for information. The CSPS then provide that information in a transparent manner. **CSA STAR consists of three layers:**
  - **Self-assessment:** Requires the release of published results 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

Vendor Management (Cont.)

Industry Standards to Consider (Cont.)

- **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?
  - CCSL provides information for the **following schemes**:
    - Certified Cloud Service
    - **CSA STAR Attestation**
    - EuroCloud Star Audit Certification
    - **ISO/IEC 27001**
    - **PCI-DSS v3**
    - Service Organization Control (SOC) 1, 2, 3
  - **Cloud Certification Schemes Metaframework (CCSM)**: An extension for the CCSL designed to provide a high-level **mapping of customer security requirements** to security objectives in existing cloud security schemes
    - **My security requirements are "X"** — which cloud security schemes align with that?

Contract Management

Managing a Contract

- Meet the **ongoing needs** of the business
- Monitor **contract performance**
- Adhere to contract terms
- **Manage** outages, incidents, violations, and variations

Key Contract Components

- Performance measurements **(metrics)**
- SLAs
- **Right to audit**
- Definitions
- Termination
- Litigation
- Assurance
- Compliance
- **Access to data**
- Cyber risk insurance

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

Supply Chain Management

Each supplier added (including CSPs and their subcontractors) **increases risk to the organization.**

To keep track of ongoing supply chain risks, a CCSP should:

- **Obtain regular updates** from vendors listing dependencies and reliance on third parties
- Challenge vendors on identified **single points of failure**
- **Continuously monitor** suppliers and their changes

Standards and Frameworks for 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

Supply Chain
Management

Preparing for the Exam

- **Study** the interactive diagram — **understand** the material so you can **reason through exam questions.**
- **Take** the practice exam several times. Get used to the **mental strain** of a long exam.
- Take advantage of the **flash cards** — use them during short study sessions.
- **Exam Details**
  - Duration: **3 hours**
  - Number of questions: **125**
  - Question format: **Multiple choice**
  - Passing score: **700 out of 1000 (70%)**

Back
Next

Back to Main

Registering for the Exam

1. Go to the Pearson Vue ISC2 page and sign in.
2. Select the **CCSP exam**.
3. Choose a **testing center**.
4. Choose a **date and time**.
5. **Pay** for your exam.
6. After you **pass your exam** (which I'm confident you will!), be sure to let us know how you did in the Linux Academy Community**.**

Good Luck!

All of us at Linux Academy are behind you 100%.

Back

Main Menu