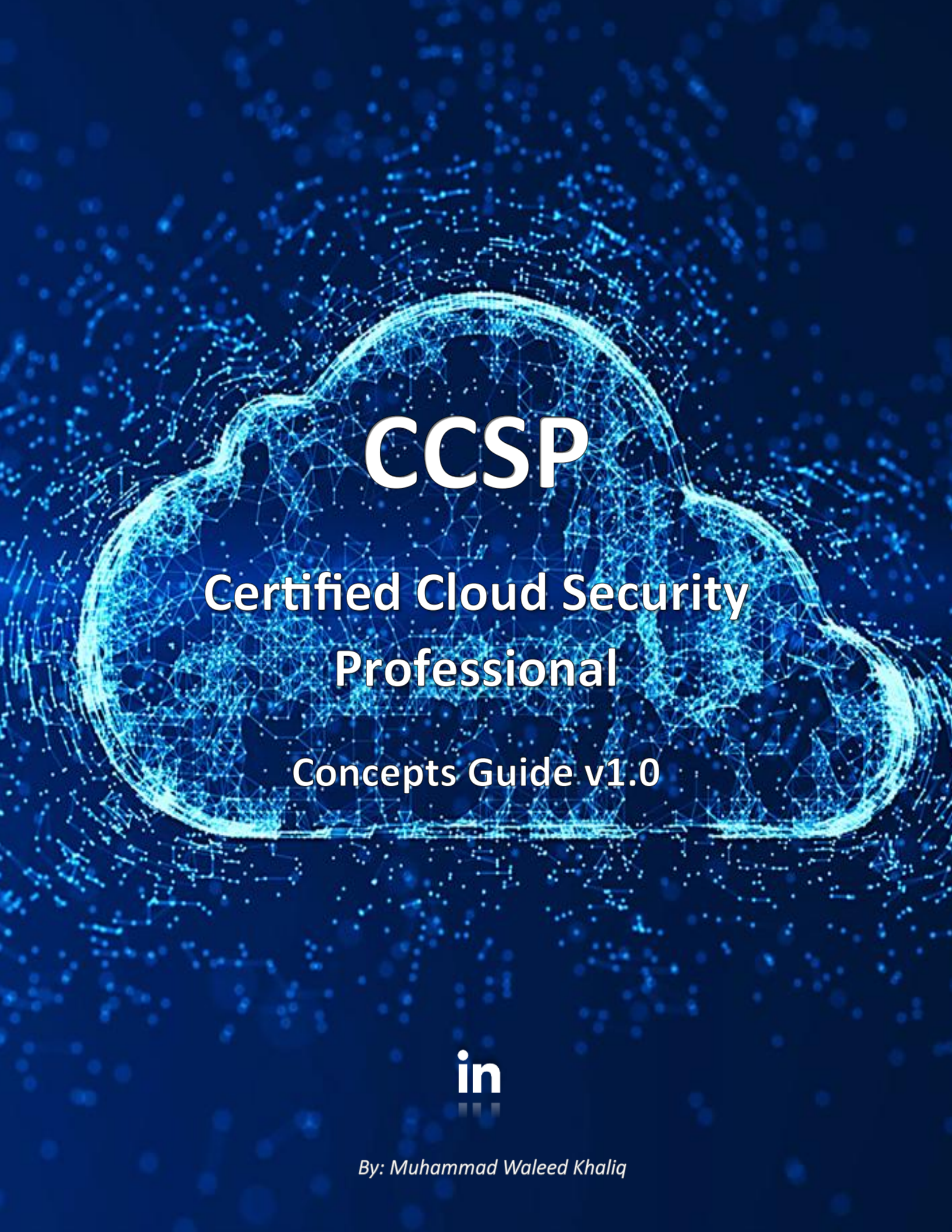


CCSP

Certified Cloud Security Professional

Concepts Guide v1.0

By: Muhammad Waleed Khaliq

Contents

Disclaimer

This study guide is intended to serve as a study resource for individuals pursuing the Certified Cloud Security Professional (CCSP) certification. While every effort has been made to ensure the accuracy of the content.

The information provided in this book is based on publicly available materials, personal expertise, and interpretation of the CCSP examination domains.

It is not affiliated with or endorsed by (ISC)², the organization that administers the CCSP certification. All trademarks and references to CCSP are the property of (ISC)².

This book is not a substitute for official (ISC)² study materials, and candidates are encouraged to consult the (ISC)² website and resources for the most accurate and up-to-date information regarding the CCSP certification

Domain 1 - Cloud Concepts, Architecture, and Design

NIST SP 800-145, cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

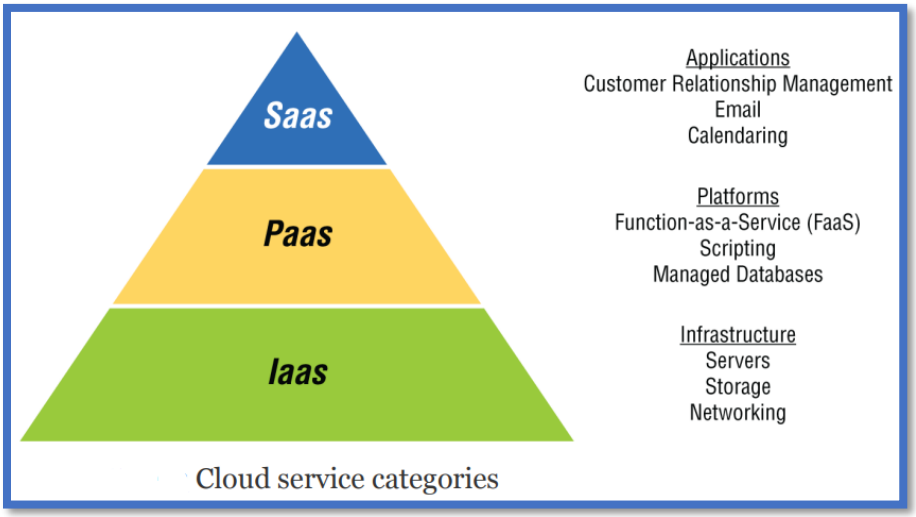
"Simply, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change."

ISO/IEC 17788, "**Cloud Computing–Overview and Vocabulary**."

- ***Cloud application:*** An application that does not reside or run on a user's device but rather is accessible via a network.
- ***Cloud application portability:*** The ability to migrate a cloud application from one cloud provider to another.
- ***Cloud computing Network-accessible platform*** that delivers services from a large and scalable pool of systems, rather than dedicated physical hardware and more static configurations.
- ***Cloud data portability:*** The ability to move data between cloud providers.
- ***Cloud deployment model*** How cloud computing is delivered through a set of configurations and features of virtual resources. The cloud deployment models are public, private, hybrid, and community.
- ***Cloud service Capabilities*** offered via a cloud provider and accessible via a client.
- ***Cloud service category*** A group of cloud services that have a common set of features or qualities.
- ***Community cloud*** A cloud services model where the tenants are limited to those that have a relationship together, with shared requirements, and are maintained or controlled by at least one member of the community.
- ***Data portability***: The ability to move data from one system or another without having to re-enter it.
- ***Hybrid cloud*** A cloud services model that combines two other types of cloud deployment models.
- ***Infrastructure as a Service (IaaS)*** A cloud service category where infrastructure level services (such as processing, storage, and networking) are provided by a cloud service provider.
- ***Interoperability***: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.
- ***Measured services*** are delivered and billed for in a metered way, to ensure that consumers only use what they are allotted.
- ***Multitenancy*** Having multiple customers and applications running within the same environment, but in a way that they are isolated from each other and oftentimes not visible to each other yet share the same resources.
- ***On-demand self-service*** A cloud customer can provision services in an automatic manner, when needed, with minimal involvement from the cloud provider.
- ***Platform as a Service (PaaS)*** A cloud service category where platform services, such as Azure or AWS, are provided to the cloud customer, and the cloud provider is responsible for the system up to the level of the actual application.

- ***Private cloud services model*** where the cloud is owned and controlled by a single entity for their own purposes.
- ***Public cloud services model*** where the cloud is maintained and controlled by the cloud provider, but the services are available to any potential cloud customers.
- ***Resource pooling:*** The aggregation of resources allocated to cloud customers by the cloud provider.
- ***Reversibility*** The ability of a cloud customer to remove all data and applications from a cloud provider and completely remove all data from their environment, along with the ability to move into a new environment with minimal impact to operations.
- ***Software as a Service (SaaS)*** A cloud service category in which a full application is provided to the cloud customer, and the cloud provider maintains responsibility for the entire infrastructure, platform, and application.
- ***Tenant*** One or more cloud customers sharing access to a pool of resources.

Cloud Service Models



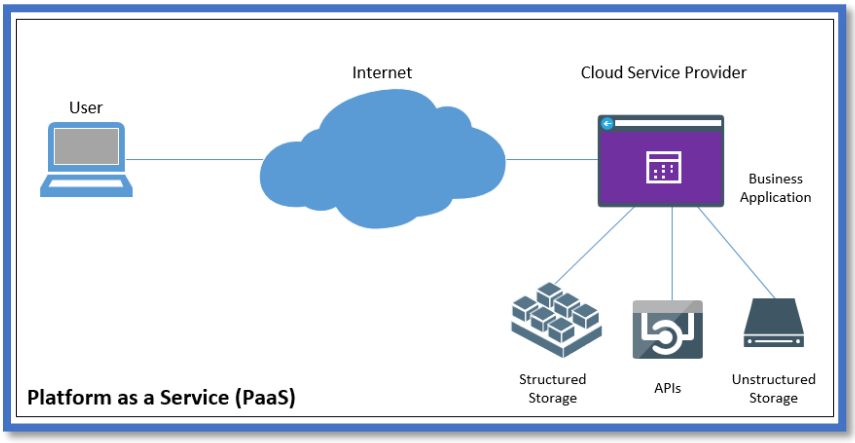
Software as a Service (SaaS) models provide fully functional applications typically accessible via a web browser. For example, Google's Gmail is a SaaS application. The vendor (Google in this example) is responsible for all maintenance of the SaaS services. Customers do not manage or control any of the cloud-based assets.

Security Concerns for SaaS

- **Data Segregation:** Customer's data can be stored in the same location with multiple tenants. Proper segregation should be implemented not only at the physical level but also at application level.
- **Data Access and policies:** Access to customer's data should be reviewed, logged, and monitored. CSP policy should match the customer's policy.
- **Web Application Security:** Given a large number of co-located tenants, if a vulnerability is exploited, CSP and customers will have a catastrophic situation.

Platform as a Service (PaaS) models provide consumers with a computing platform, including hardware, operating systems, and a runtime environment. The runtime environment includes programming languages, libraries, services, and other tools supported by the vendor. Customers deploy applications that they've created or acquired, manage their applications, and possibly modify

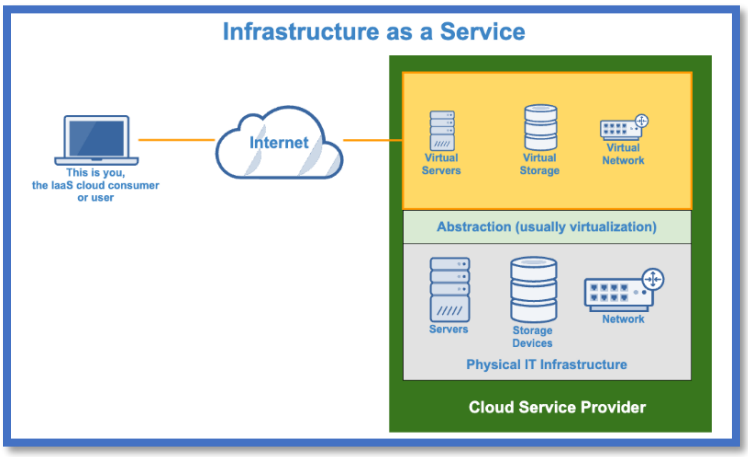
some configuration settings on the host. However, the vendor is responsible for maintenance of the host and the underlying cloud infrastructure.



Security Concerns for PaaS

- **System and resource isolation:** Should not have shell/root access of the servers running. Admin should be segmented.
- **User-level permission:** Each instance should have its own permission. We need to ensure no authorization creep is there (accumulating privileges over time).
- **User access management:** Helps to protect CIA of an asset. Key components are:
  - **Intelligence:** Collection, analysis, auditing, and reporting based on organization policies.
  - **Administration:** On-boarding/off-boarding or changing account access on system.
  - **Authentication:** Multi-factor authentication should be enabled.
  - **Authorization:** Least privilege should always be applied.
- **Protection against malware, backdoors, and trojans:** Once the backdoor is created, it creates a permanent attack surface.

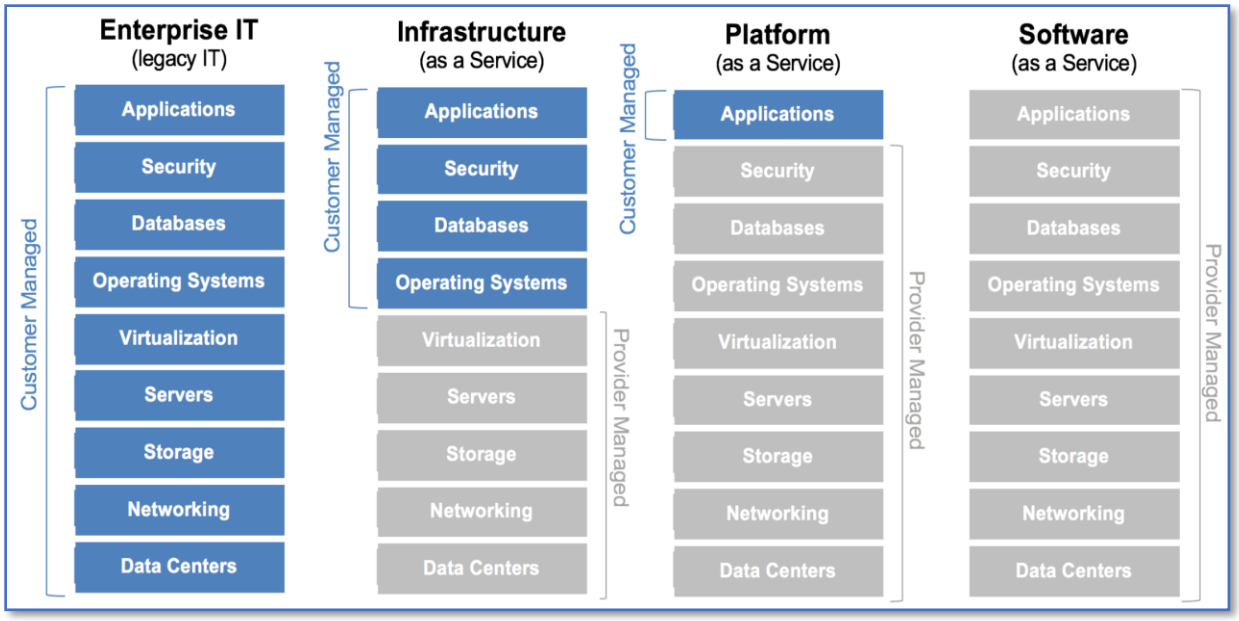
Infrastructure as a Service (IaaS) models provide basic computing resources to customers. This includes servers, storage, and networking resources. Customers install operating systems and applications and perform all required maintenance on the operating systems and applications. The vendor maintains the cloud-based infrastructure, ensuring that consumers have access to leased systems.



Security Concerns for IaaS

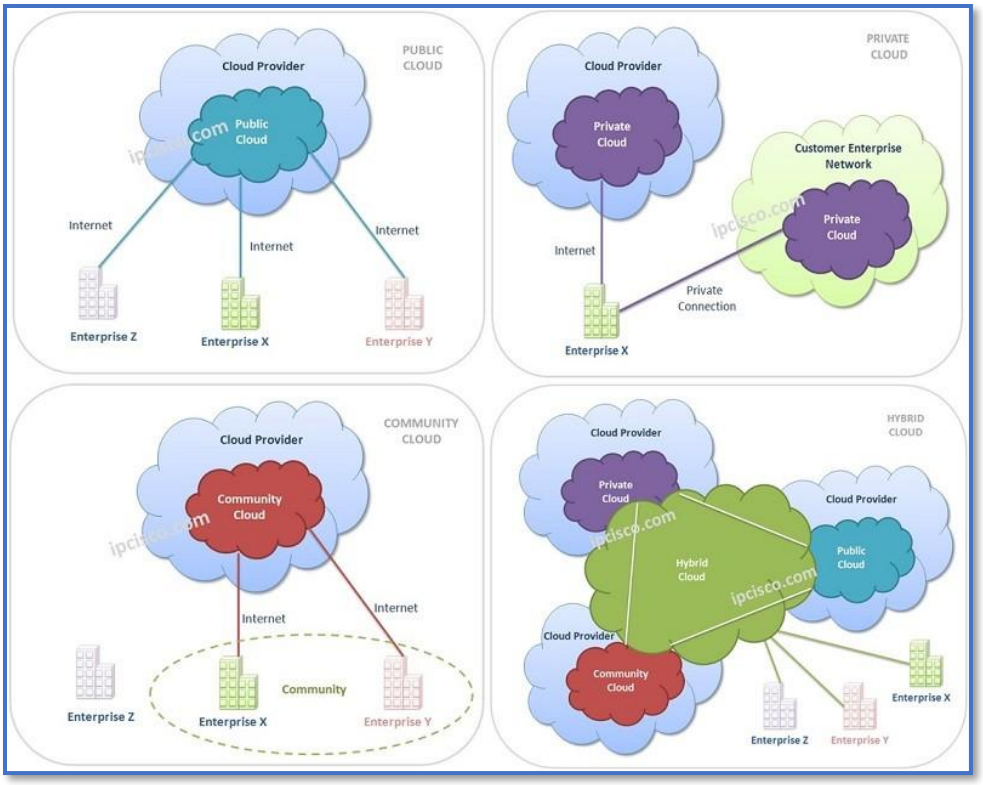
- **VM attacks:** VMs on the same physical machine can attach to each other because they share the same Hardware and Software resources (Hypervisor).
- **Virtual Network:** It contains virtual switch software that controls the traffic between virtual NIC and physical NIC.
- **Hypervisor attacks:** Compromising hypervisors will give control over VMs. Common attacks are:
  - Hyper-jacking: Installing rogue hypervisor that can take complete control.
  - VM escape: Crashing the guest OS to get out of it and running an arbitrary code in the host OS. This allows malicious VM to take control over the host OS.
- **VM Based Rootkits**: Installing malicious hypervisors on the fly or manipulation to gain control.
- **Virtual Switch attacks:** Modification of switch configuration, VLAN, and trusted zone and ARP tables.
- **DoS Attacks:** Misconfiguration at the hypervisor can make one VM utilize all the resources making other VMs unavailable.
- **Colocation:** Multiple VMs residing on a single server and sharing the same resources increases the attack surface and risk of VM to VM and VM to Hypervisor compromise.
- **Multitenancy:** Information leakage, VM to VM and VM to Hypervisor compromise.
- **Loss of control:** Users don't have control over the location of the data centers and services, and CSP is not aware of the content which they run.
- **Network topology:** Due to a lot of changes in cloud (VMs are being added or removed or moved from one host to another) creates a challenge for network topologies.
- **Logical network segmentation:** Isolation is important for sensitive information. VLAN, NAT, Bridging etc.
- **No physical endpoints:** Due to virtualization, physical endpoints (switches, servers, NIC) have been reduced.
- **Single Point of Access:** Hosts have limited NIC to all VMs.

IaaS	PaaS	SaaS
Scalability	Auto-scaling	Support costs and efforts
Cost of ownership of physical hardware	Multiple host environments	Reduced overall costs
High availability	Choice of environments	No licensing obligations
Physical security requirements	Flexibility	Ease of use and administration
Location and access independence	Ease of upgrades / Access	Standardization
Metered usage	Cost effective	
	Relief from licensing obligations	



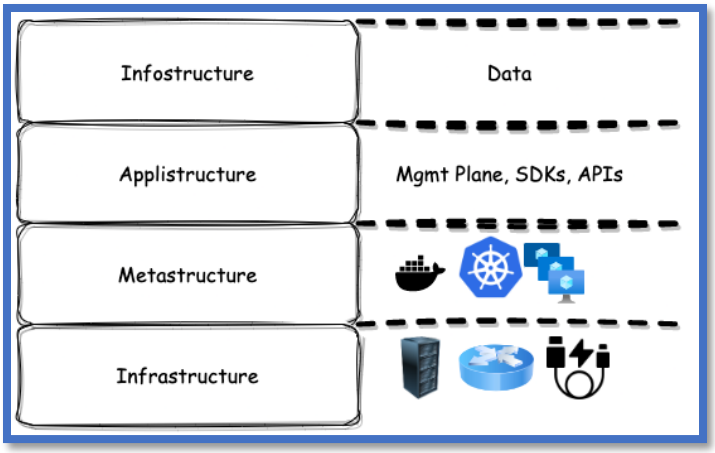
Cloud Deployment Models

- ***Public cloud*** includes assets available for any consumers to rent or lease and is hosted by an external CSP. Service-level agreements can effectively ensure that the CSP provides cloud-based services at a level acceptable to the organization.
- ***Private cloud*** deployment model is used for cloud-based assets for a single organization. Organizations can create and host private clouds using their own on-premises resources. If so, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party for exclusive use of the organization. Maintenance requirements are typically split based on the service model (SaaS, PaaS, or IaaS).
- ***Community cloud*** deployment model provides cloud-based assets to two or more organizations that have shared concerns, such as a similar mission, security requirements, policy, or compliance considerations. Assets can be owned and managed by one or more of the organizations. Maintenance responsibilities are shared based on who is hosting the assets and the service models.
- ***Hybrid cloud*** models include a combination of two or more clouds that are bound together by a technology that provides data and application portability. Similar to a community cloud model, maintenance responsibilities are shared based on who is hosting the assets and the service models in use.
- ***Vertical Cloud*** refers to a cloud that is specialized to meet the specific needs of a particular vertical (industry). All the functions are options provided by the CSP are tailored to meet industry use.



Cloud Logical Model

- **Infrastructure:** The core components of a computing system: compute, network, and storage. The foundation that everything else is built on.
- **Metastructure:** The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.
- **Infostructure:** The data and information. Content in a database, file storage, data warehouses and data lakes, Business Intelligence (BI) etc.
- **Applistructure:** The applications deployed in the cloud and the underlying application services used to build them. For example, Platform as a Service features like message queues, artificial intelligence analysis, RESTful APIs or notification services.
- **Software-Defined Infrastructure (SDI)** refers to an IT framework where all aspects of infrastructure—compute, storage, and networking—are virtualized and managed through software, rather than traditional hardware-based configuration and control. SDI provides agility, scalability, and automation by decoupling hardware from the management and operational layers, enabling a more flexible and dynamic infrastructure.



TIP Application security maps to applistructure, data security to infostructure, and infrastructure security to infrastructure. *The key difference between cloud and traditional computing is the metastructure.*

Cloud Secure Data Lifecycle

- **Create** – data is generated from cloud-based services.
- **Store** – data is maintained online within the cloud.
- **Use** – data is accessed as part of program execution.
- **Share** – data must be available to all authorized users.
- **Archive** – data must be preserved in long-term storage when necessary.
- **Destroy** – data should be permanently and securely removed from a system when it is no longer needed.

Cloud Security Process Model

- Identify necessary security and compliance requirements, and any existing controls.
- Select your cloud provider, service, and deployment models.
- Define the architecture.
- Assess the security controls.
- Identify control gaps.
- Design and implement controls to fill the gaps.
- Manage changes over time.

Cloud Computing Roles based on ISO/IEC 17788:

- ***Cloud auditor:*** An auditor that is specifically responsible for conducting audits of cloud systems and cloud applications.
- ***Cloud service broker*** A partner that serves as an intermediary between a cloud service customer and cloud service provider.
- ***Cloud service customer*** One that holds a business relationship for services with a cloud service provider.
- ***Cloud service partner*** One that holds a relationship with either a cloud service provider or a cloud service customer to assist with cloud services and their delivery. cloud auditor, cloud service broker, and cloud service customer all under the umbrella of cloud service partners.
- ***Cloud service provider*** One that offers cloud services to cloud service customers.

- ***Cloud service user*** One that interacts with and consumes services offered to a cloud service customer by a cloud service provider.
- ***Cloud Service Integrator (CSI)*** is a company or individual that specializes in helping organizations adopt and utilize cloud computing services. CSIs act as intermediaries between cloud service providers (CSPs) and their customers, offering a range of services to facilitate the transition to cloud.
- ***Cloud Carrier,*** also known as a cloud network provider or cloud connectivity provider, is a telecommunications company that specializes in providing network connectivity and infrastructure for cloud computing environments.
- ***Cloud Developer*** is a software engineer who specializes in designing, developing, and maintaining applications and services that run on cloud computing platforms.
- ***Cloud Security Architect*** is a cybersecurity professional responsible for designing, implementing, and managing security solutions for cloud computing environments.
- ***Cloud Regulator*** is a government agency or regulatory body that oversees and regulates the cloud computing industry.

Cloud Computing Key Characteristics:

- ***On demand self-service:*** Although it comes with a risk as people can provision themselves without using approved transaction methods.
- ***Broad Network Access:*** Information should be available at any point from anywhere. Challenges are using mobile devices, as no security controls are present.
- ***Resource Pooling:*** Ensuring ideal resources are adequately distributed among the customers to have full utilization.
- ***Rapid Elasticity:*** Allow users to obtain additional resources, space, etc. as required to meet the workload. If this is done locally, Capex is high.
- ***Measured Service:*** Resources are metered and logged for billing and utilization reporting. E.g. Pay as you use.
- ***Tertiary site***, also known as a disaster recovery site or hot site, is a fully equipped facility that can be used to restore operations in the event of a disaster. Unlike a cold site, which requires significant setup time, a tertiary site is ready to be activated immediately.

Cloud Service Customer

The cloud service customer performs the following roles:

- ***Cloud service user*** Uses the cloud services.
- ***Cloud service administrator*** Tests cloud services, monitors service, administers security of services, provides usage reports on cloud services, and addresses problem reports.
- ***Cloud service business manager*** Oversees business and billing administration, purchases the cloud services, and requests audit reports, as necessary.
- ***Cloud service integrator*** Connects and integrates existing systems and services to the cloud.

Cloud Service Provider

The cloud service provider performs the following roles:

- ***Cloud service operations manager*** Prepares systems for the cloud, administers services, monitors service, provides audit data when requested or required, and manages inventory and assets.

- ***Cloud service deployment manager*** Gathers metrics on cloud services, manages deployment steps, and processes, and defines the environment and processes.
- ***Cloud service manager*** Delivers, provisions, and manages the cloud services.
- ***Cloud service business manager*** Oversees business plans and customer relationships as well as processes financial transactions.
- ***Customer support and care representative*** Provides customer service and responds to customer requests.
- ***Inter-cloud provider Responsible*** for peering with other cloud services and providers as well as overseeing and managing federations and federated services.
- ***Cloud service security and risk manager*** Manages security and risks and oversees security compliance.
- ***Network provider*** Responsible for network connectivity, network services delivery, and management of network services.

Cloud Service Partner

The cloud service partner performs the following roles:

- ***Cloud service developer*** Develops cloud components and services and performs the testing and validation of services.
- ***Cloud reseller*** is a business or individual that partners with cloud service providers to sell cloud-based solutions to end users.
- ***Cloud auditor*** Performs audits as well as prepares and authors audit reports.
- ***Cloud service broker*** Obtains new customers, analyzes the marketplace, and secures contracts and agreements.

Emerging Cloud Service Categories

- ***Compute as a Service (CaaS)*** allows for the execution of compute-intensive workloads to be performed in the cloud. Code can be executed in a serverless environment where the customer only pays for the computing time and cycles they consume, without the need for setting up server instances or environments.
- ***Database as a Service (DBaaS)*** is a subscription service where the database is installed, configured, secured, and maintained by the cloud provider, with the cloud customer only responsible for loading their schema and data.
- ***Desktop as a Service (DaaS)*** is a cloud-based equivalent of a traditional virtual desktop interface (VDI) that is hosted and managed by a cloud provider rather than on hardware owned by the customer.
- ***Identity as a Service (IDaaS)*** is a subscription-based service for identity and access management (IAM) and single sign-on (SSO) that is offered over the Internet versus deployed by the customer.
- ***Network as a Service (NaaS)*** is a cloud-based virtual network where customers can quickly and easily change network configurations via software versus the traditional need for cabling and hardware appliances.
- ***Security as a Service (SECaaS)*** enables companies to contract with an external vendor to supply and manage their security operations for such technologies as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), data loss prevention (DLP), and anti-virus implementations.

- ***Storage as a Service (STaaS)*** is a cloud service where the provider offers storage space and solutions on a subscription service. Cloud customers incur costs based on the amount of storage that is consumed or reserved.

Cloud Shared Considerations

- ***Interoperability:*** It defines how easy it is to move or reuse application components regardless of provider, platform, OS; application component work together etc.
- ***Portability:*** Key aspect in selecting CSP as it can help in preventing vendor lock-in.
- ***Availability:*** Systems and resources availability defines the success and failure of CSP. There should not be a single point of failure (SPOF) and should have at least 99.9% availability.
- ***Security:*** Should be a part of a contractual agreement stating minimum security requirement. CSP also have a NDA signed.
- ***Privacy:*** It's a significant challenge for CSP and customers as there's no uniform privacy law. Should be a part of the contract and SLA. EU countries have it included in EU Data Protection Law (Now GDPR).
- ***Resiliency:*** Cloud infrastructure continues to operate in the event of disruption or disaster.
- ***Performance:*** Cloud computing and performance should go hand in hand. Should focus on Network, Compute, Storage, and Data (Design, integration and development activities)
- ***Governance:*** Process and decision to define and assign responsibilities and verify performance.
- ***SLA:*** If CSP fails to provide services at the decided time, the financial stipulation should be invoked.
- ***Auditability:*** Access to report and obtain evidence. It gives customer the confidence while choosing CSP.
- ***Regulatory Compliance:*** Organization's requirement to adhere to relevant regulations (e.g. PCI-DSS, HIPAA etc.).
- ***Maintenance and Versioning:*** Versioning changes can be tracked and tested, with known versions available to fall back to if necessary due to problems with new versions.
- ***Reversibility:*** is the ability of a cloud customer to take all their systems and data out of a cloud provider and have assurances from the cloud provider that all the data has been securely and completely removed within an agreed-upon timeline.

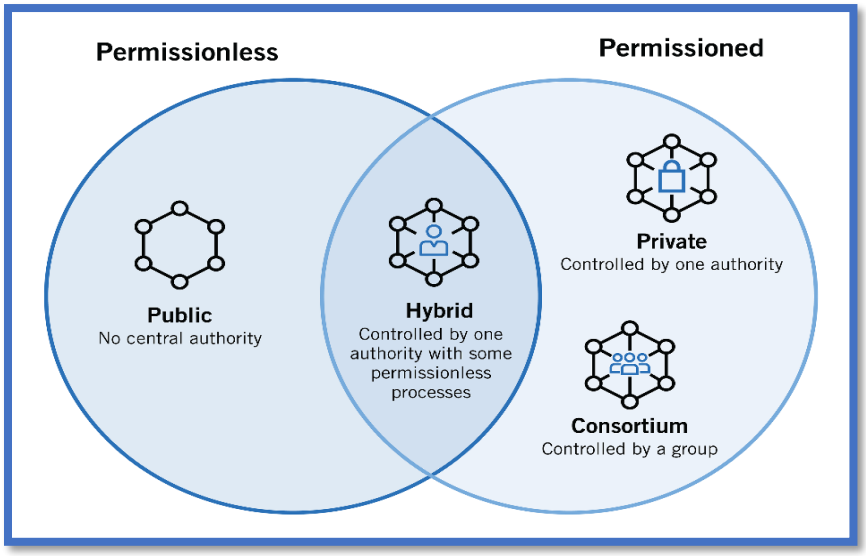
Impact of Related Technologies

- ***Artificial intelligence (AI)*** allows machines to learn from processing experiences, adjusting to new data inputs and sources, and ultimately perform human-like analyses and adaptations to them. here are three main types of artificial intelligence: analytical, human-inspired, and humanized.
  - **Human-inspired AI** is an advanced subset of artificial intelligence that integrates cognitive and emotional intelligence, aiming to replicate human-like decision-making, reasoning, and adaptability.
  - **Analytical AI** focuses on learning from data to identify patterns, make predictions, and support decision-making. It excels in handling structured and unstructured data and is primarily designed to solve complex problems by analyzing vast amounts of information without mimicking human emotions or creativity.
  - **Humanized AI** refers to artificial intelligence designed to emulate human behavior, reasoning, and emotional intelligence to create more natural and relatable interactions with people.

AI Analytics Types

- **Descriptive analytics:** Describe and summarize data to understand past and current trends.
- **Predictive analytics**: Use historical data and statistical models to forecast future events.
- **Prescriptive analytics**: Provide recommendations for optimal decision-making based on simulations and modeling.

- ***Machine learning*** involves using scientific and statistical data models and algorithms to allow machines to adapt to situations and perform functions that have not been explicitly programmed to perform.
- **Cognitive cloud computing** is a fusion of artificial intelligence (AI) and cloud computing. It involves leveraging cloud-based infrastructure to deliver cognitive services, such as natural language processing, machine learning, and image recognition. These services enable computers to understand, learn, and interact with the world in ways that mimic human cognition.
- ***Blockchain*** is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system. It contains every single record of each transaction. Types of block chain:
  - Public Blockchain: No central authority, non-restrictive, permission-less.
  - Private Blockchain: Controlled by authority
  - Hybrid Blockchain: Combination of the private and public blockchain.
  - Consortium Blockchain: Controlled by group



Quantum computing is a revolutionary technology that harnesses the principles of quantum mechanics to perform calculations exponentially faster than classical computers. Unlike classical computers, which use bits (0 or 1) to represent information, quantum computers use qubits (quantum bits) that can exist in multiple states simultaneously, allowing for parallel processing and solving complex problems that are intractable for classical machines.

Data Science is an interdisciplinary uses scientific methods, algorithms, processes, and systems to extract knowledge and insights from structured and unstructured data. Key components of data science are:

- Data Collection

- Data Preparation
- Data Analysis
- Machine Learning
- Data Visualization

Internet of Things (IoT) refers to the network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity capabilities that enable them to collect, exchange, and act on data. These devices communicate with each other, cloud systems, and users through the internet, creating a connected ecosystem that improves efficiency, automation, and decision-making.

Cloud Security Models:

- ***Conceptual models or frameworks*** include visualizations and descriptions used to explain cloud security concepts and principles, such as the CSA logical model in this document.
- ***Controls models or frameworks*** categorize and detail specific cloud security controls or categories of controls, such as the CSA CCM.
- ***Reference architectures*** are templates for implementing cloud security, typically generalized (e.g. an IaaS security reference architecture). They can be very abstract, bordering on conceptual, or quite detailed, down to specific controls and functions.
- ***Design patterns*** are reusable solutions to particular problems. In security, an example is IaaS log management. As with reference architectures, they can be more or less abstract or specific, even down to common implementation patterns on particular cloud platforms.

Security Concepts Relevant to Cloud Computing

Cryptography

- Encryption
  - Data in Transit (SSL, TLS)
  - Data at Rest (AES 256)
  - Key Management
    - Remote Key Management Service – maintained by customer at their own location; provides full control to the cloud customer.
    - Client-Side Key Management Service – in SaaS implementations, it is provided by the cloud provider but controlled by the customer.

Access control (authentication & authorization)

- Account Provisioning & Deprovisioning
- Directory Services (LDAP)
- Administrative and Privileged Access (Auditing, SOD)
- Authorization (defining the permissions i.e., allow/grant and/or deny)

Data and media sanitation: moving from one data center to another (cloud providers included)– it is always imperative that data be properly and completely cleansed from any storage system.

- Vendor Lock-in for Data – cloud customer is bound to a particular provider.
- Data Sanitization
  - Overwriting (known as the "zeroing")
  - Cryptographic erasing (destruction of the keys)

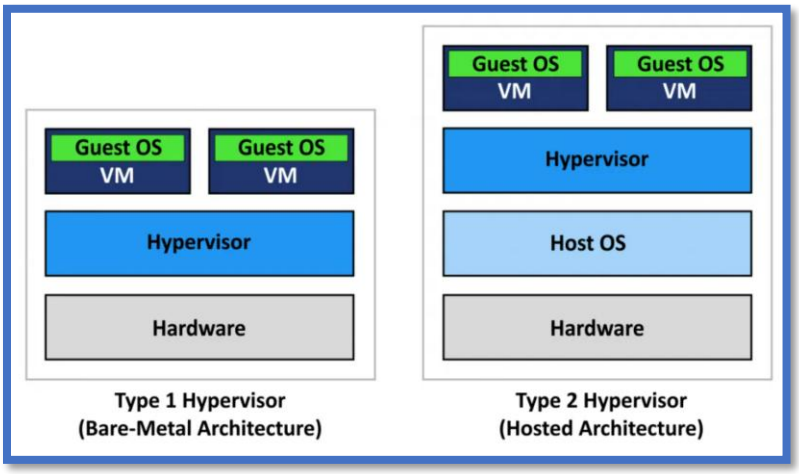
Network security

- Network Security Groups
  - Traffic Inspection: inspecting the contents of data packets

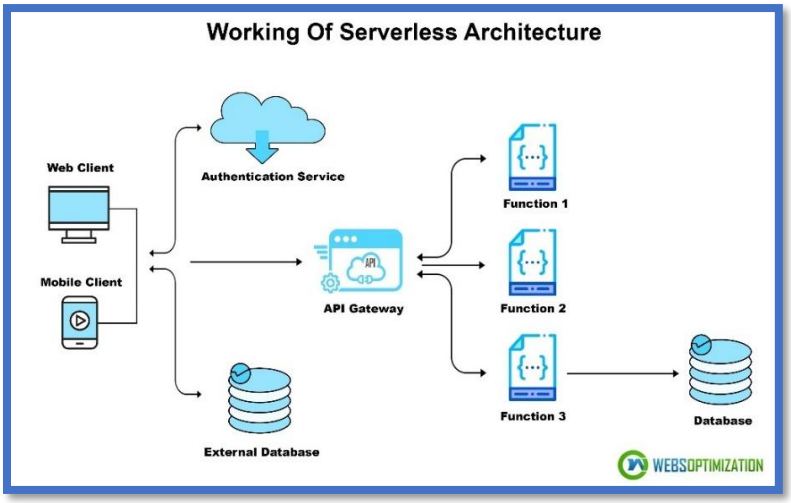
- Geofencing: is a location-based service that creates a virtual geographic boundary around a specific area using technologies like GPS, RFID, Wi-Fi, or cellular data. When a device enters or exits this predefined boundary, certain actions or notifications are triggered.
- Zero Trust Network: principle of automatically trusting no users or processes coming into or out of a network. In order to gain access, users must be authenticated, authorized, and validated against security policies during all transactions.

Virtualization security

- Type 1 Hypervisor – bare-metal deployment; no host operating system
- Type 2 Hypervisor – virtualization is software-based; host OS is required.

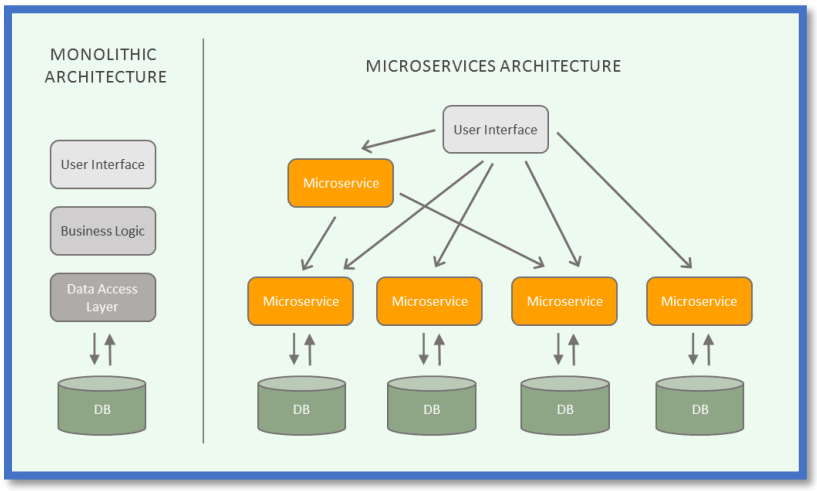


- **Container Security:** the process of implementing security tools and policies to assure that all in your container is running as intended, including protection of infrastructure, software supply chain, runtime, and everything between.
- **Ephemeral Computing:** the practice of creating a virtual computing environment as a need arises and then destroying that environment when the need is met, and the resources are no longer in demand.
- **Serverless Technology:** serverless provider allows users to write and deploy code without the hassle of worrying about the underlying infrastructure.



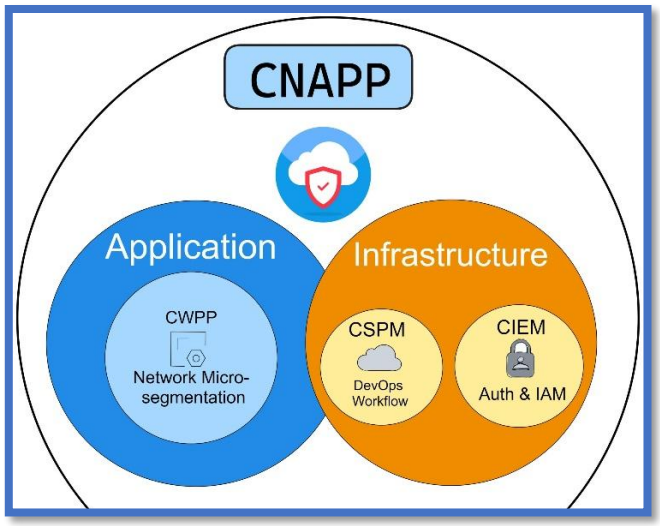
Cloud Native Microservices Architecture (CNMs): When a number of **microservices** are deployed in the cloud environment to handle specific operations in a collective manner, they can be classified as Cloud Native Software (CNS) or Cloud Native Applications (CNAs). CNA development is completely based on the CI/CD DevOps model rather than a traditional waterfall model.

Monolithic: Traditional application design is often called "monolithic" because the whole thing is developed in one piece. Even if the logic of the application is modular, it's deployed as one group.



Cloud Native Application Protection Platform (CNAPP) is a combination of tools in a single platform designed to provide agility, security, visibility, flexibility, and compliance with cost optimization to manage and protect cloud infrastructure.

- **Cloud security posture management (CSPM)** to monitor, identify, alert on, and remediate compliance risks and misconfigurations in cloud environments.
  - **Infrastructure as code** security to detect misconfigurations in code early in the software development life cycle to prevent vulnerabilities at runtime.
  - **Compliance and governance** to manage compliance status as well as remediate configuration drift and policy violations across multicloud environments.
- **Cloud infrastructure entitlement management (CIEM)** to mitigate the risk of data breaches in public clouds by continuously monitoring permissions and activities.
  - **Data protection** to monitor, classify, and inspect data and prevent exfiltration of critical data as a result of phishing, malicious insiders, or other cyberthreats.
  - **Identity and access management** (IAM) to control access to internal resources, ensuring users' permissions grant them appropriate access to systems and data.
- **Cloud workload protection platforms (CWPP)** to provide visibility and control for physical machines, VMs, containers, and serverless workloads in hybrid, multicloud, and data center environments.



Zero Trust enforces the concept of granular access privileges based on identities and their roles to implement and enforce authorization. Users, systems, and applications are granted access after the continuous verification of identities based on authentication and authorization. Simple rule "**never trust, always verify**".

- **Zero Trust Architecture (ZTA)**
- **Zero Trust Network Access (ZTNA)**
- **Zero Trust Security (ZTS)**

Zero Trust Principle

- Verify explicitly. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
- Use least privilege access. Limit user access with just-in-time and just-enough-access (JIT and JEA), risk-based adaptive policies, and data protection.
- Assume breach. Segment access to minimize scope of impact. Verify end-to-end encryption, use analytics to get visibility, drive threat detection, and improve defenses.

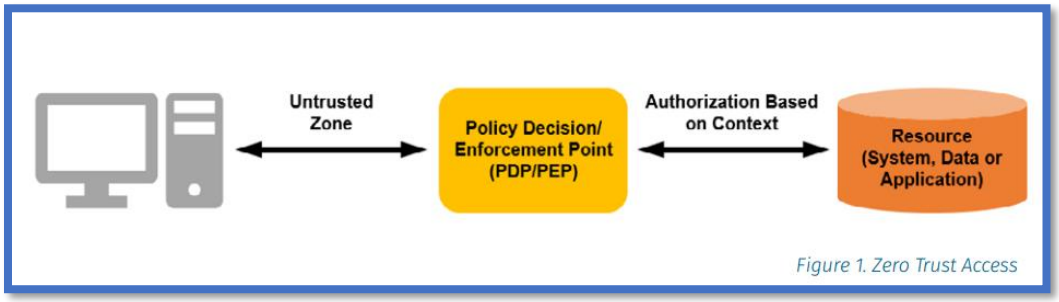
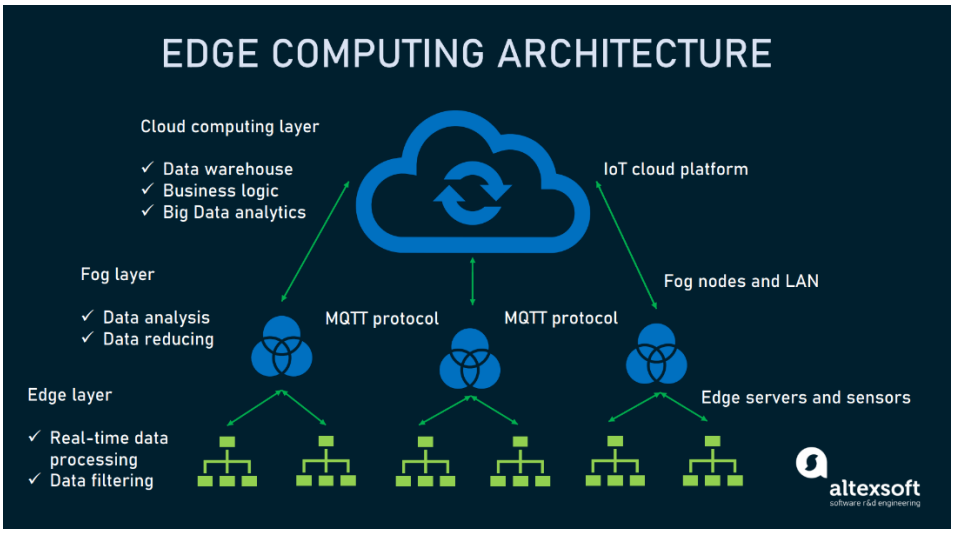


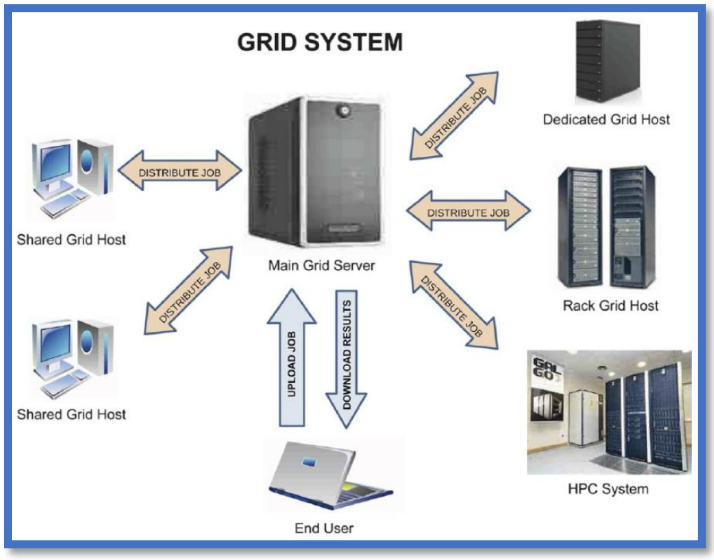
Figure 1. Zero Trust Access

Edge computing is a location-specific computer model in which data is processed closer to the source. This means data processing, including computation, takes place closer to the user for better efficiency and at a faster speed. The goal of edge computing is to minimize latency by bringing public cloud capabilities to the edge.

Fog computing is a decentralized computing infrastructure that extends cloud computing capabilities to the edge of the network. It allows data processing, storage, and analysis closer to the data source, which can improve response times and save bandwidth.



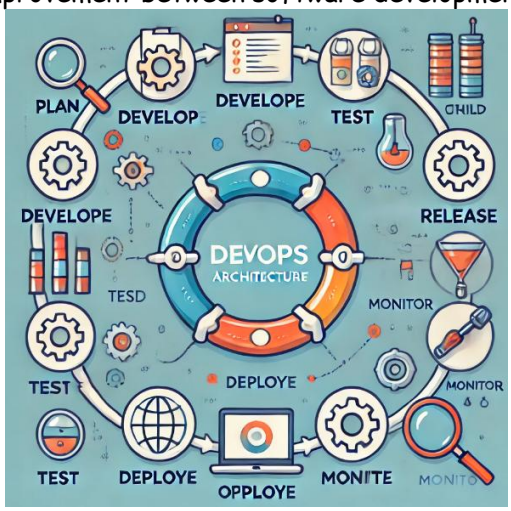
Grid Computing is a distributed architecture of multiple computers connected to solve complex problems. Unlike traditional networks that primarily focus on communication between devices, grid computing harnesses the unused processing cycles of connected computers to solve a problem that is too complex for any stand-alone machine. The computers are either directly connected or through scheduling systems.



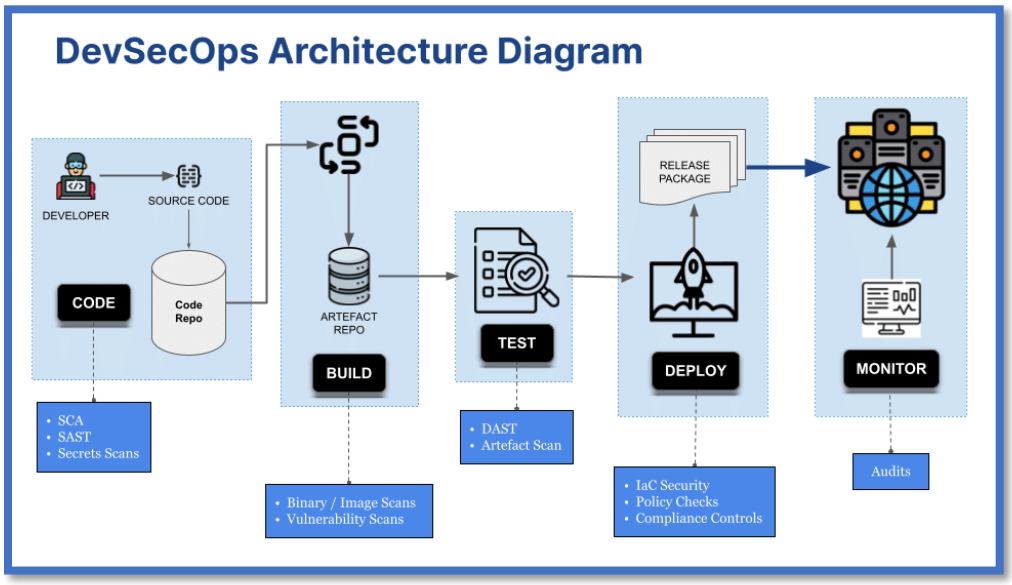
Confidential computing refers to cloud computing technology that can isolate data within a protected central processing unit (CPU) while it is being processed. Within the CPU's environment there is the data that the CPU processes and the methods used to process this data.

Trusted Execution Environments (TEEs) are hardware-based security mechanisms that create a secure enclave within a device, isolating sensitive data and code from the rest of the system. TEEs provide a trusted environment where sensitive operations can be performed without the risk of unauthorized access or tampering.

DevOps is a set of practices and cultural philosophies that aim to shorten the development life cycle and provide continuous delivery of high-quality software. It emphasizes collaboration, automation, and continuous improvement between software development and IT operations teams.



DevSecOps is a security-focused extension of DevOps that integrates security practices throughout the entire software development lifecycle (SDLC). It emphasizes collaboration between development, operations, and security teams to ensure that security is built into software from the beginning, rather than being an afterthought.



Common threats (The CSA Egregious 11)

1. Data breaches: unauthorized exposure of sensitive and private data.
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access, and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs

8. Weak control plane
9. **Metastructure** failure: the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. **Applistructure** failures: the applications deployed in the cloud and the underlying application services used to build them
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

Security Hygiene

- **Baselines:** are sets of standards and settings applied to systems when they are first built. They are essentially templates and images built to security policies and are applied to any systems based on their purpose.
- **Patching:** Over time, software is updated with new features, bug fixes, and security fixes.

Cloud-based Business Continuity/Disaster Recovery Planning

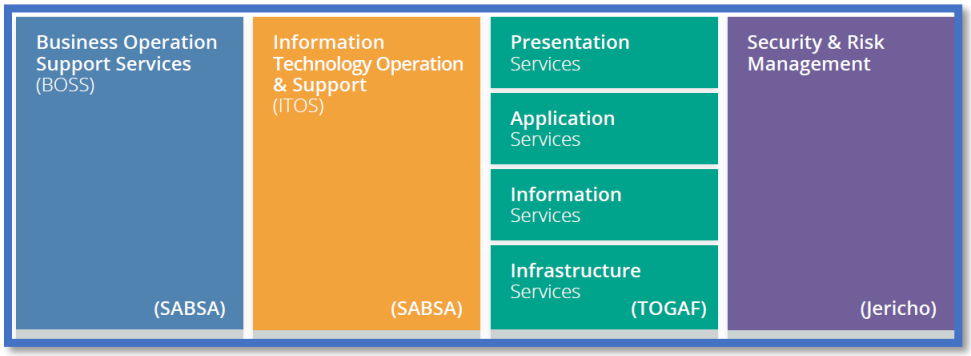
- Elements (Confidentiality, Integrity, and Availability)
- Critical Success Factors
  - Knowing the customer's responsibilities vs. the CSP's responsibilities
  - Knowing that these continuity and disaster recovery components that are covered by the SLA
- Important SLA Components
  - No single point of failure
  - Migration to alternate systems should be possible within agreed-upon timeframes
  - Automated controls should be available to verify data integrity
  - Regular assessment of the SLA should be carried out.
- Cost-Benefit Analysis – is performed when considering a cloud deployment
- Resource Pooling and Cyclical Demands – to satisfy business requirements
- Data Center Costs vs. Operational Expense Costs
- Focus Change – cloud technology is different from traditional IT
- Ownership and Control – loss of control over data
- Cost Structure

Cloud Security Alliance Enterprise Architecture

1. **Business Operation Support Services (BOSS)** focuses on the nontechnical aspects of an organization that are central to cloud security and operations. This includes legal, compliance, and human resources considerations.
2. **Information Technology Operation & Support (ITOS)** focuses on service delivery, concepts fall under this area such as change management, project management, release management, configuration management, and asset management.
3. **Technology Solution Services (TSS**) focuses on the multitiered architecture of applications and how they securely operate together:
   - **Presentation services** These are for the actual interaction with the user, either through a website or an application.
   - **Application services** These services sit behind the presentation tier and perform operations for the user with the underlying data. This is where code written by the developers is actually implemented and executed.

- **Information services** These are the databases or files that contain the actual data for the application accessed from the application tier.
- **Infrastructure services** These are the underlying hardware or hosting infrastructure for all applications and IT services. They can be virtual machines, applications, databases, and networks as well as the physical infrastructure and facilities that host them.

4. **Security and Risk Management (SRM):** SRM is what most people think of when it comes to cybersecurity. It includes authentication and authorization data as well as the auditing systems and tools to ensure their compliance. SRM also includes pen testing, vulnerability scanning, and ethical hacking.



Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a cybersecurity framework designed specifically for cloud environments. It provides a set of controls to help organizations assess and manage cloud security risks while aligning with industry standards and best practices. It has 17 domains.

Domain	Description
AIS (Application & Interface Security)	Protects APIs and user interfaces from unauthorized access and vulnerabilities.
AAC (Audit Assurance & Compliance)	Ensures compliance with industry regulations and internal policies.
BCR (Business Continuity & Resilience)	Focuses on disaster recovery, fault tolerance, and resilience in cloud environments.
CCC (Change Control & Configuration Management)	Manage changes to cloud configurations to maintain security.
DCS (Data Security & Information Lifecycle Management)	Ensures secure data handling, encryption, and lifecycle management.
ECS (Encryption & Key Management)	Defines standards for encryption and secure key management.
GRM (Governance, Risk, and Compliance)	Establishes policies and risk management strategies.
IAM (Identity & Access Management)	Controls access to cloud systems, ensuring secure authentication and authorization.
IVS (Infrastructure & Virtualization Security)	Secures cloud infrastructure and virtual environments.
SEC (Security Incident Management)	Outlines processes for detecting, responding to, and mitigating security incidents.
STA (Supply Chain Management)	Manages risks associated with third-party services and supply chains.
TVM (Threat and Vulnerability Management)	Identifies and mitigates threats and vulnerabilities in the cloud.

UEM (Universal Endpoint Management)	Secures endpoint devices accessing cloud resources.
HRS (Human Resources Security)	Ensures personnel are trained and monitored for secure cloud operations.
IPY (Interoperability & Portability)	Facilitates seamless data and service portability across cloud providers.
SEF (Security & Encryption Functions)	Ensures encryption mechanisms comply with industry standards.
MCA (Mobile Cloud Applications)	Addresses risks unique to mobile applications running on the cloud.

SANS Cloud Security Principles

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. E-mail and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Networking Monitoring and Defense
14. Security Awareness and Skills training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration testing

Well-Architected Framework

- **Reliability** The system can recover from failures and continue to operate.
- **Security** Data and applications are protected from threats.
- **Cost Optimization** The most value is gotten from the money spent.
- **Operational Excellence** Production systems run as expected and meet business needs.
- **Performance Efficiency** Systems can adapt to fluid demands in workload.
- **Sustainability** Environmental impacts from computing resources are minimized.

Sherwood Applied Business Security Architecture (SABSA)

- Business Requirements Engineering Framework (known as Attributes Profiling)
- Risk and Opportunity Management Framework
- Policy Architecture Framework
- Security Services-Oriented Architecture Framework
- Governance Framework
- Security Domain Framework
- Through-Life Security Service Management & Performance Management Framework

IT Infrastructure Library (ITIL)

- ITIL Service Strategy
- ITIL Service Design
- ITIL Service Transition
- ITIL Service Operation
- ITIL Continual Service Improvement

The Open Group Architecture Framework (TOGAF)

- Common language and communications
- Standardizing on open methods and technologies to avoid proprietary lock-in
- Utilizing resources more effectively and efficiently to save money
- Demonstrating return on investment

NIST 800-145 - The NIST Definition of Cloud Computing
NIST SP 800-146 – Cloud Computing Synopsis and Recommendations
NIST SP 500-293 – USFG Cloud Computing Technology Roadmap (Volumes I-III)
NIST 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations:

- Insider threats and malicious activity
- Software application security, including web-based applications and APIs
- Social networking
- Mobile devices
- Cloud computing
- Persistent threats
- Privacy
- Access control
- Identity and authentication

NIST 500-293 – Guide, framework how to migrate to cloud
NIST 800-292 – Cloud Reference Architecture
NIST 800-64 - SDLC
NIST 800-37 - Risk management
NIST 800-61 - Incident Response

ISO/IEC 27001:2013

The latest 2013 revision contains a group of 114 controls organized under the following 14 control domains:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance

- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ISO/IEC 27017 is a globally recognized standard that provides guidelines for information security controls specific to cloud computing environments. It is an extension of ISO/IEC 27002 and is designed to address the unique risks associated with cloud services, for both cloud service providers (CSPs) and cloud customers. The overall standard also covers the following 18 sections, which go into more depth on cloud services:

1. Scope
2. Normative references
3. Definitions and abbreviations
4. Cloud sector-specific concepts
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communications security
14. System acquisition, development, and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance

Service organization controls (SOC)

International Standard for Attestation Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*. SSAE 18 and ISAE 3402 engagements are commonly referred to as ***service organization controls (SOC)*** audits, and they come in three forms:

SOC 1 Engagements Assess the organization's controls that might impact the accuracy of financial reporting.

SOC 2 Engagements Assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. SOC 2 audit results are confidential and are normally only shared outside the organization under an NDA.

SOC 3 Engagements Assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. However, SOC 3 audit results are intended for public disclosure.

SOC Reports

	SOC-1	SOC-2	Notes
Type-1	Point in time financial audit.	Point in time security, availability, or processing integrity of either a system or the information the system processes.	Allowed to display the SOC logo. Shows good faith to customers. Not as meaningful as a Type 2.
Type-2	Over a period of time financial audit.	Over a period of time audit of security, availability, or processing integrity of either a system or the information the system processes.	Allowed to display the SOC logo. Trusted by your customers. Must be repeated periodically.

SOC 1 reports focuses on the kinds of information that would be relevant and pertinent to a financial audit of an organization and its financial statements. This report includes information about the management structure of the organization, the targeted client and customer base, as well as information about the regulations the organization is subjected to and the auditors that verify compliance.

SOC 2 reports expand beyond basic financial audit primers to include five areas. The one most important to the Cloud Security Professional is the security principle (the others are availability, processing integrity, confidentiality, and privacy). The security principles include seven categories:

- Organization and management
- Communications
- Risk management and design implementation of controls
- Monitoring of controls
- Logical and physical access controls
- System operations
- Change management

Information and Data Governance Types

- **Information classification** – What is the high-level description of valuable information categories (such as highly confidential, regulated)?
- **Information management policies** – What activities are allowed for different information types?
- **Location and jurisdictional policies** – Where can data be geographically located? What are the legal and regulatory implications or ramifications?
- **Authorizations** – Who is allowed to access different types of information?
- **Custodianship** – Who is responsible for managing the information at the bequest of the owner?

Common Criteria is an ISO/IEC international standard for computer security certification. It carries the designation of ISO/IEC 15408.

ITSEC	CC	Security Evaluation
0	EAL1	Functional Tested
1	EAL2	Structural Tested
2	EAL3	Methodically tested and proofed
3	EAL4	Methodically developed, tested and proofed
4	EAL5	Semiformal developed and tested
5	EAL6	Semiformal verification of the design
6	EAL7	Formal verification of the design

FIPS 140-2 standard establishes the security requirements for cryptographic hardware and software used to protect sensitive but unclassified information. It defines four levels of security. They are aptly called Levels 1–4, with increasing levels of requirements and scrutiny:

Level 1 Provides the lowest level of security. The only requirements are based on the cryptographic modules being used, and at least one on the approved list must be present. There are no physical security requirements at Level 1.

Level 2 Requires role-based authentication where a cryptographic module is used for actual authentication processes. The module must also have mechanisms that show evidence of any attempts to tamper with it.

Level 3 Requires physical protection methods to ensure a high degree of confidence that any attempts to tamper are evident and detectable. It requires the cryptographic module to not only authenticate the user to the system but also to verify authorization.

Level 4 Provides the highest level of security and tamper detection. The criteria at Level 4 is that any attempts to tamper will be detected and prevented and any data that is clear text will be zeroed should a tamper be successful. Level 4–certified modules are very useful in systems that lack physical security protections and need to rely more on data protections.

FIPS 140-2 standard is divided into 11 sections that define security requirements:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self-tests
10. Design Assurance
11. Mitigation of Other Attacks

ISO/IEC 27034- defines an application security management process (ASMP)

Data Roles

Data Subject: Refers to any individual person who can be identified, directly or indirectly, via an identifier. Identifiers may include name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Data Steward: is a role within an organization responsible for ensuring the accuracy, consistency, and quality of data. They play a crucial role in maintaining data integrity, particularly in large enterprises with complex data landscapes.

Data Owner: is the individual or entity within an organization that has the ultimate responsibility for a specific dataset. They are typically senior executives or department heads who have the authority to make decisions about the data, including its use, access, and retention.

Data Custodian: is the individual or entity responsible for the technical aspects of managing and protecting data. They are often IT professionals who are tasked with implementing and maintaining the systems and processes that store, protect, and access data.

Data Processor: is an entity that processes personal data on behalf of a data controller. This can include a wide range of activities, such as collecting, storing, organizing, adapting, retrieving, consulting, using, disclosing, transmitting, or otherwise processing personal data.

Data Controller: The person or entity that controls processing of the data.

Key management covers the entire lifecycle of keys beginning to end including:

- Generation
- Communication and distribution
- Storage
- Use
- Revocation
- Destruction

Key Recovery

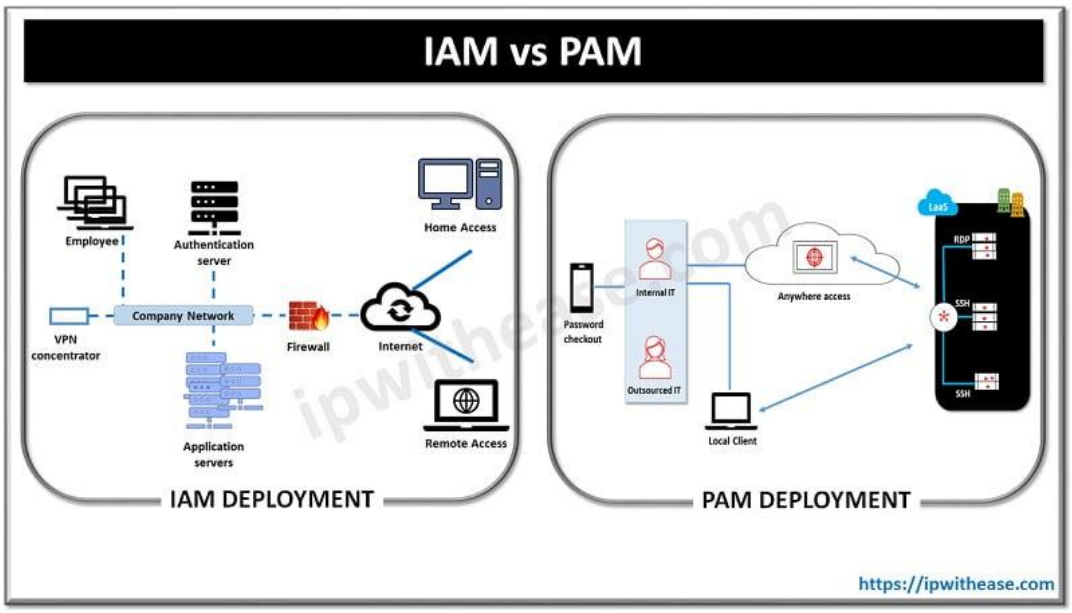
Circumstances where you need to recover a key for a particular user, without that user's cooperation, such as in termination or key loss.

Key Escrow

Copies of keys held by a trusted third party in a secure environment, which can aid in many of the other areas of key management.

Identity and access management (IAM) is a system to identify and authorize users across an organization.

Privileged Access Management (PAM) is a subset of IAM that focuses on privileged accounts and systems.


IAM vs PAM
Employee
Authentication server
Home Access
Company Network
VPN concentrator
Firewall
Internet
Application servers
Remote Access
IAM DEPLOYMENT
Password checkout
Internal IT
Outsourced IT
Anywhere access
Local Client
LaaS
RDP
SSH
SSH
PAM DEPLOYMENT
https://ipwithease.com

Domain 2 – Cloud Data Security

Data Management Life Cycle

Data dispersion refers to a technique used in cloud computing environments of breaking data into smaller chunks and storing them across different physical storage devices. Cloud based data dispersion also implements erasure coding to allow for reconstruction of data if some segments are lost.

Erasure refers to the process of securely removing or deleting data to ensure it cannot be accessed, reconstructed, or used in any way.

- **Overwriting**:
  - Replacing existing data with random or specific patterns multiple times to make recovery impossible. Tools: DBAN (Darik's Boot and Nuke), CCleaner, or built-in OS utilities.
- **Cryptographic Erasure**:
  - Deleting the encryption keys used to secure data, rendering the data inaccessible.
- **Physical Destruction**:
  - Physically destroying storage media, such as shredding hard drives or incinerating discs.
- **Factory Reset**:
  - Restoring devices to their original state, often used in smartphones or IoT devices.
- **Degaussing**:
  - Using a magnetic field to disrupt data on magnetic storage media like hard drives or tapes.

Data flows are serverless data-processing managed services through cloud providers and are designed to allow customers to upload their pipeline code.

Cloud Data Storage Architectures

IaaS – self-service (by customer) administration of an online environment

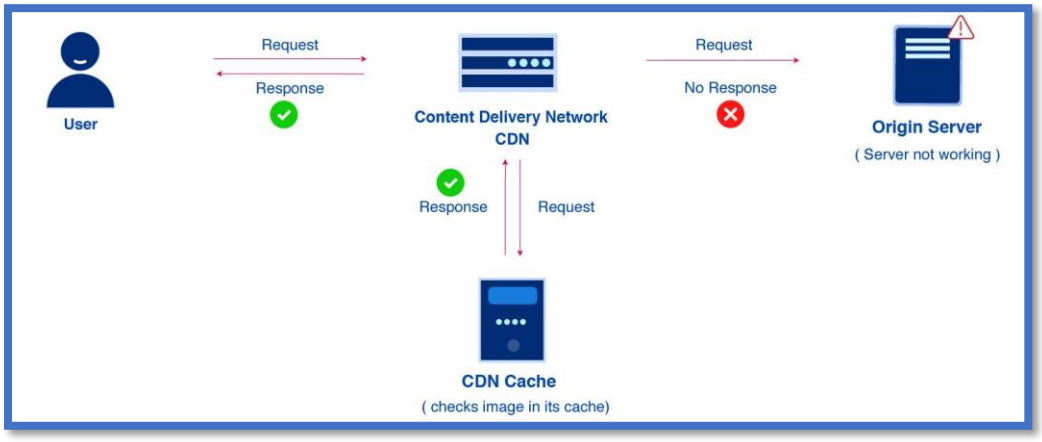
- Volume/Block Storage – type of storage that provides a logical, block-level view of data.
- It's often used to store data for virtual machines, databases, and other applications.
- Object – identifies files that are given a key value (tokenization) for access, like a file share.
- Uses metadata to retrieve files.
- Raw device mapping (RDM)- is a form of virtualization that allows a particular cloud VM to access a storage logical unit number (LUN). The LUN is a dedicated portion of the overall storage capacity for use by a single VM, and RDM provides the method for a VM to access its assigned LUN.

PaaS – DevOps

- Structured – data stored in a relational database; highly organized. Structured data is often accompanied by a description of its format known as a data model or schema, which is an abstract view of the data's format in a system.
- Binary Large Object (blob) or Unstructured data: Blobs are unstructured data; that is to say, data that does not adhere to a particular data model like the columns in a database. multimedia files, text files, and Microsoft Office files

SaaS – (Gmail, Google Apps, Office 365, Hotmail)

- Information Storage and Management – data is entered via a web interface (API) and stored in a back-end database (based on volumes and objects)
- Content and File Storage – data stored within the applications
- Content delivery network (CDN) – data stored as objects and distributed to geographically dispersed nodes to improve performance.



Ephemeral storage is short term in nature, unstructured, and only available and in existence while a cloud service instance requires it. Once that node is shut down or removed, the storage associated with it is also destroyed.

Block Storage (aka Volume Storage) is a type of data storage commonly used in cloud computing and enterprise environments. It divides data into fixed-sized blocks (chunks), each with a unique identifier, which allows data to be stored and retrieved independently. It is designed for high-

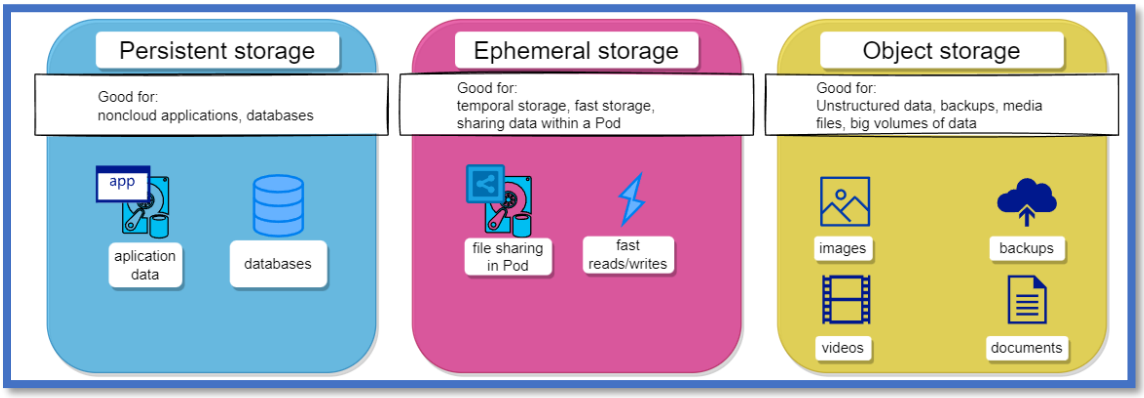
performance applications and is often used for databases, virtual machines, and transactional systems.

Aspect	Block Storage	File Storage	Object Storage
Structure	Fixed-sized blocks	Hierarchical files and folders	Data stored as objects with metadata
Performance	High-speed and low latency	Moderate	Lower compared to block storage
Use Case	Databases, VMs, transactional systems	Shared storage, collaboration tools	Archiving, backup, media storage
Sharing	Typically, one-to-one (single instance)	One-to-many (multi-instance sharing)	Unlimited sharing
Scalability	Highly scalable, but at higher costs	Scalable, but limited to file systems	Massively scalable
Access Protocols	Direct (block device drivers)	NFS, SMB	RESTful APIs

File Storage is a type of data storage that organizes and stores information in a hierarchical file-and-folder structure, similar to how files are organized on a computer. It is commonly used for shared file systems, collaboration, and applications that require centralized access to files.

Persistent storage is any data storage device that retains data after power to that device is shut off. It is also sometimes referred to as nonvolatile storage.

Object storage is a storage technology used for unstructured data, which eliminates the scaling limitations of traditional file storage.



Threats to Storage

- ***Malware and Ransomware:*** Malicious software that encrypts or corrupts data, often demanding payment for recovery. Example: Ransomware attacks targeting cloud storage.
- ***Data Breaches:*** Unauthorized access to sensitive data due to weak security controls. Example: Exploiting vulnerabilities in storage APIs.
- ***Man-in-the-Middle (MitM) Attacks:*** Intercepting data during transfer to storage systems. Example: Unauthorized parties capturing unencrypted data.
- ***Insider Threats:*** Malicious or negligent actions by employees or contractors with access to storage systems. Example: Deleting or copying sensitive files.
- ***Hardware Failures:*** Malfunctioning hard drives, SSDs, or storage arrays causing data loss. Example: Wear and tear leading to bad sectors on drives.

- ***Natural Disasters:*** Events like floods, earthquakes, or fires damaging physical storage facilities. Example: Data center flooding without sufficient disaster recovery planning.
- ***Theft or Vandalism:*** Physical theft of servers or damage to storage devices. Example: A stolen external hard drive containing critical data.
- ***Accidental Deletion:*** Users mistakenly deleting files or overwriting important data. Example: Misconfigured backup procedures leading to permanent data loss.
- ***Improper Configuration:*** Mismanagement of storage settings leading to vulnerabilities. Example: Leaving a cloud storage bucket publicly accessible.
- ***Data Corruption:*** Mistakes during data transfers or storage operations causing corruption. Example: Incomplete writing processes during power outages.
- ***Data Tampering or Unauthorized access:*** Unauthorized modification of stored data, compromising its integrity. Example: Altering financial records stored in a database.
- ***Denial of Service (DoS) Attacks:*** Flooding storage systems with traffic to render them inaccessible. Example: Targeted attacks on a cloud provider's storage services.
- ***Metadata Manipulation:*** Tampering with file metadata to mislead or disrupt storage operations. Example: Changing timestamps or access permissions.
- ***Shared Tenancy Risks:*** Vulnerabilities arising from multi-tenant environments in cloud storage. Example: Data leakage between tenants due to misconfigured isolation.
- ***Account Hijacking:*** Unauthorized access to cloud storage accounts through phishing or stolen credentials. Example: Hackers gaining access to a business's cloud storage through compromised logins.
- ***Lack of Data Portability:*** Challenges in migrating data between cloud providers leading to potential loss. Example: Vendor lock-in restricting access during a provider outage.
- ***Non-Compliance:*** Failing to meet data protection regulations such as GDPR, HIPAA, or CCPA. Example: Storing unencrypted sensitive customer data in violation of regulations.
- ***Data Residency Issues:*** Storing data in locations with conflicting legal requirements. Example: Cross-border data storage violating local privacy laws.

Design and Apply Data Security Strategies

Encryption – driven by compliance requirements:

- Data in Motion: IPsec and TLS (VPNs)
- Data at Rest: storage vs. archival encryption like full disk encryption e.g. bit locker (AES 256)
- Data in Use: Information and Data Rights Management (IRM, DRM)

Challenges with Encryption

- The integrity of encryption is dependent on key management and how they are secured (CSP control vs. Customer)
- Encryption can be challenging to implement effectively when a CSP is required to process the encrypted data. This is true even for simple tasks such as indexing and the gathering of metadata.
- Data in the cloud is highly portable. It replicated, is copied, and is backed up extensively, making encryption and key management challenges.
- Multitenant cloud environments and the shared use of physical hardware present challenges for the safeguarding of keys in volatile memory such as random-access memory (RAM) caches.
- Secure hardware (HSM) for encrypting keys may not exist in cloud environments, with software-based key storage often being more vulnerable.

- Storage-level encryption is typically less complex and can be more easily exploited and compromised, given sufficient time and resources. The higher you go up toward the application level, the more challenging the complexity to deploy and implement encryption becomes. However, encryption implemented at the application level is typically more effective at protecting the confidentiality of the relevant assets or resources.
- Encryption can negatively affect performance, especially high-performance data processing mechanisms such as data warehouses and data centers.
- The nature of cloud environments typically requires customer to manage more keys than traditional environments (access keys, API keys, encryption keys, and shared keys, among others).
- Some cloud encryption implementations require all users and service traffic to go through an encryption engine. This can result in availability and performance issues both to end users and to providers.
- Throughout the data lifecycle, data can change locations, format, encryption, and encryption keys. Using the data security lifecycle can help document and map all those different aspects.
- Encryption affects data availability. Encryption complicates data availability controls such as backups, disaster recovery planning (DRP), and colocations because expanding encryption into these areas increases the likelihood that keys may become compromised. In addition, if encryption is applied incorrectly within any of these areas, the data may become inaccessible when needed.
- Encryption does not solve data integrity threats. Data can be encrypted and yet be subject to tampering or file replacement attacks. In this case, supplementary cryptographic controls such as digital signatures need to be applied, along with nonrepudiation for transaction-based activities.

Encryption Implementations

- **Storage Level Encryption** – Where storage-level encryption is utilized, the encryption engine is located on the storage management level, with the keys usually held by the CSP.
- **Volume Storage Encryption** – Volume storage encryption requires that the encrypted data reside on volume storage. This is typically done through an encrypted container, which is mapped as a folder or volume. Instance-based encryption allows access to data only through the volume OS and therefore provides protection against the following:
    - Physical loss or theft
    - External administrator(s) accessing the storage
    - Snapshots and storage-level backups being taken and removed from the system
- **Instance-based encryption:** When instance-based encryption is used, the encryption engine is located on the instance itself. Keys can be guarded locally but should be managed external to the instance.
- **Proxy-based encryption:** When proxy-based encryption is used, the encryption engine is running on a proxy instance or appliance. The proxy instance is a secure machine that handles all cryptographic actions, including key management and storage. The proxy maps the data on the volume storage while providing access to the instances.
- **Object Storage Encryption**: The majority of object storage services offer server-side storage-level encryption. This kind of encryption offers limited effectiveness, with the

recommendation for external mechanisms to encrypt the data prior to its arrival within cloud environments.

- **File-level encryption:** Examples include IRM and DRM solutions, both of which can be effective when used in conjunction with file hosting and sharing services that typically rely on object storage. The encryption engine is commonly implemented at the client side and preserves the format of the original file.
- **Application-level encryption:** The encryption engine resides in the application that is utilizing the object storage. It can be integrated into the application component or by a proxy that is responsible for encrypting the data before going to the cloud. The proxy can be implemented on the customer gateway or as a service residing at the external provider.
- **Database-level encryption** may be performed at a file level by encrypting database files or may utilize transparent encryption, which is a feature provided by the database management system (DBMS) to encrypt specific columns, whole tables, or the entire database. TDE (Transparent Data Encryption) is an example.

Key Management

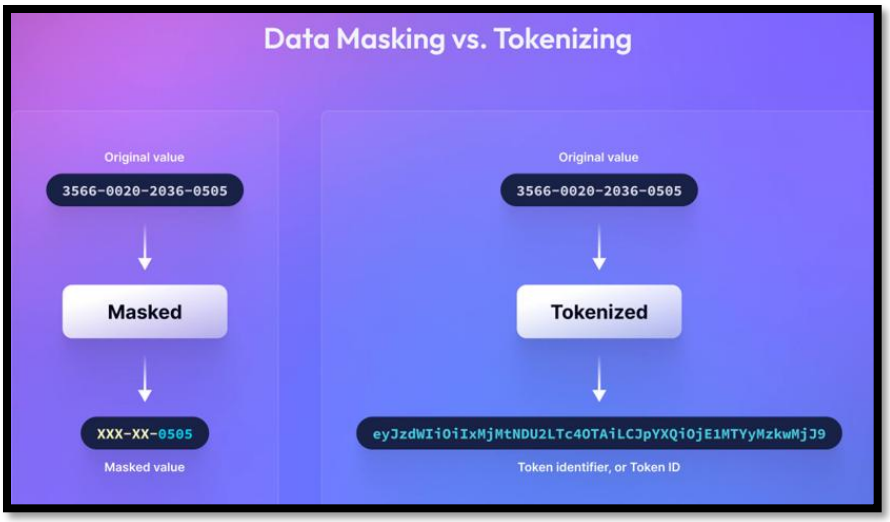
- **Access to the keys:** Leading practices coupled with regulatory requirements may set specific criteria for key access, along with restricting or not permitting access to keys by CSP employees or personnel.
- **Key storage:** Secure storage for the keys is essential to safeguarding the data. In traditional in-house environments, keys were able to be stored in secure dedicated hardware. This may not always be possible in cloud environments.
- **Backup and replication:** The nature of the cloud results in data backups and replication across a number of different formats. This can affect the ability for long- and short-term key management to be maintained and managed effectively.

TIP:

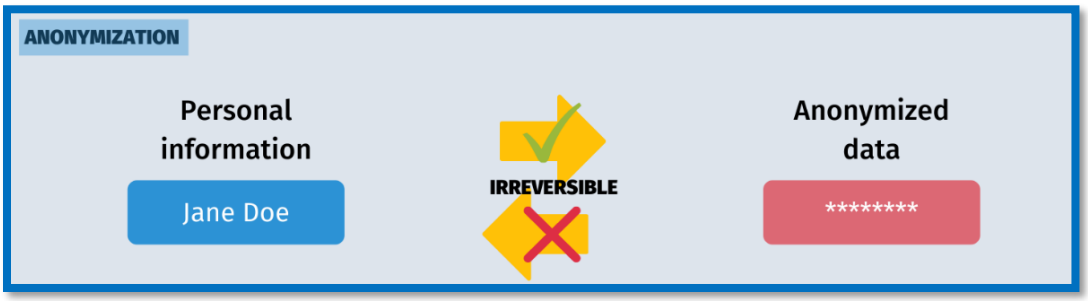
Hashing, sometimes known as *one-way encryption*, is a tool primarily associated with the integrity principle of the CIA triad. **Collision** occurs when two different inputs produce the same hash.

Masking is a data security technique used to protect sensitive information by replacing it with fictional or scrambled data while maintaining its usability. It ensures that unauthorized users cannot access sensitive data while still allowing the data to be used for testing, development, analytics, or training purposes. Examples: Social Security Numbers (SSNs), credit card details, or patient records

Tokenization replaces sensitive data, such as credit card numbers or personal identification information, with a unique, meaningless string of characters called a **token**.



Anonymization: is the process of removing or modifying personal information from data sets so that individuals cannot be readily identified.



Pseudonymization is a data privacy technique that involves replacing personally identifiable information (PII) with a unique identifier, or pseudonym.

Aggregation: *Summarizing data so that individual entries are not distinguishable.*

Data Obfuscation

- **Substitution** works by swapping out some information for other data.
- **Shuffling** involves moving data around.
- **Value variance** applies mathematical changes to primarily numerical data like dates, accounting or finance information, and other measurements.
- **Deletion or nullification** simply replaces the original data with null values.
- ***De-identifying data*** is primarily used when the data contains PII, known as *direct identifiers*, or contains information that could be combined with other data to uniquely identify an individual, known as *indirect identifiers*.

Key Management Considerations

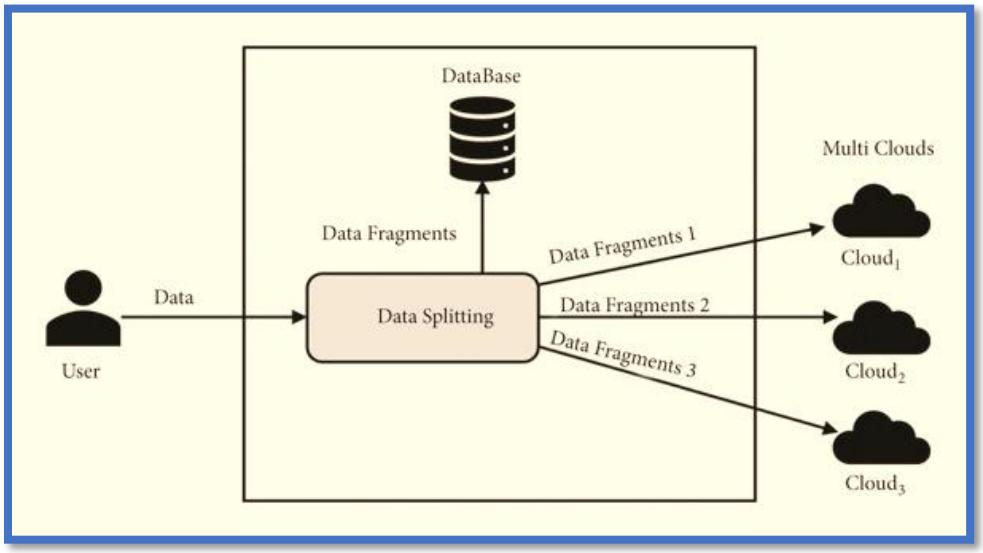
- Random number generation should be conducted as a trusted process.
- Throughout the lifecycle, cryptographic keys should never be transmitted in the clear; they should always remain in a trusted environment.
- When considering key escrow or key management "as a service," carefully plan to consider all relevant laws, regulations, and jurisdictional requirements.
- Lack of access to the encryption keys will result in lack of access to the data. This should be considered when discussing confidentiality threats versus availability threats.
- Where possible, key management functions should be conducted separately from the CSP to enforce separation of duties and force collusion to occur if unauthorized data access is attempted.

Key Storage in the Cloud

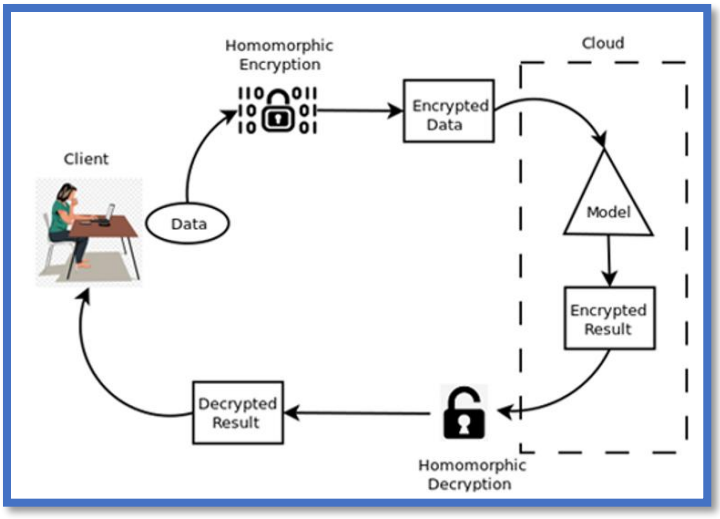
- **Internally managed:** In this method, the keys are stored on the virtual machine or application component that is also acting as the encryption engine. This type of key management is typically used in storage-level encryption, internal database encryption, or backup application encryption. This approach can be helpful for mitigating against the risks associated with lost media.
- **Externally managed:** In this method, keys are maintained separate from the encryption engine and data. The actual storage can be a separate instance (hardened especially for this specific task) or on a hardware security module (HSM).
- **Managed by a third party:** This is when a trusted third party provides key escrow services.

Emerging Technologies

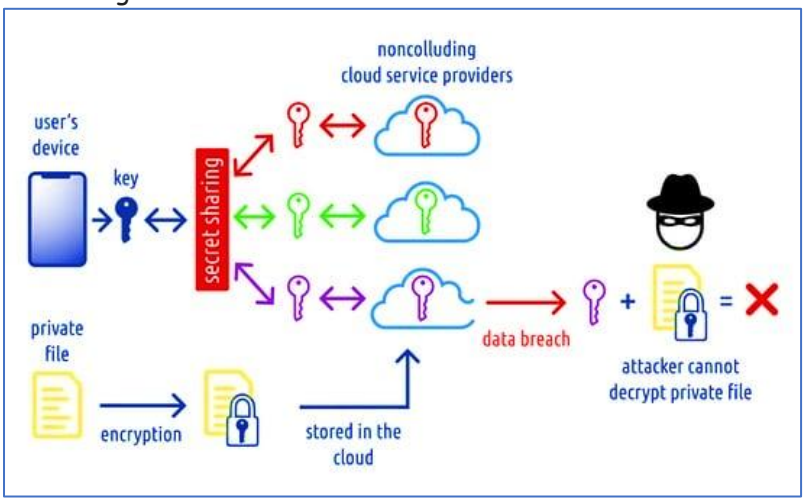
- **Bit splitting**: involves splitting up and storing encrypted data or information across different cloud storage, stronger confidentiality mechanisms.



- **Homomorphic encryption**: is a cryptographic method that enables computations to be performed directly on encrypted data without requiring access to the underlying plaintext. The results of these computations, when decrypted, match the outcome of operations performed on the original plaintext data. This unique capability makes homomorphic encryption particularly useful for secure data processing in sensitive or regulated environments, such as finance, healthcare, and cloud computing.

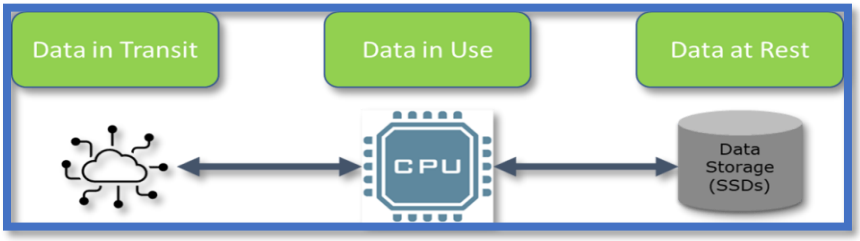


- ***Secret Sharing Made Short (SSMS)*** is a cryptographic protocol used for distributing a secret (such as a password or cryptographic key) among a group of participants. Each participant receives a "share" of the secret, and only a specific combination of these shares can reconstruct the original secret.



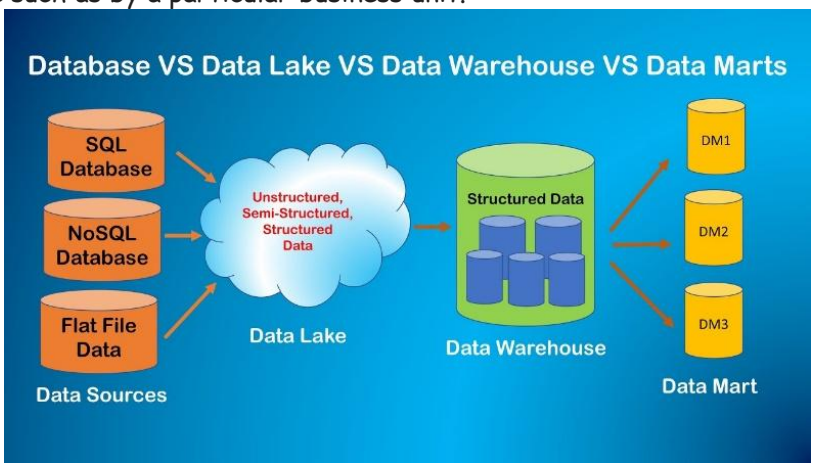
Data States

- **Data at rest (DAR),** systems holding the data, which can be servers, desktops, workstations, mobile devices, and storage.
- **Data in transit (DIT)**, traffic as it leaves the network through various protocols, such as HTTP/ HTTPS and SMTP.
- **Data in use (DIU),** data that is currently being updated, processed, erased, accessed, or read by a system.



Data Discovery – emphasizes interactive, visual analytics rather than static reporting; goal is to enable users to find meaningful information in data. Data discovery is being driven by these trends:

- **Data lake** is an unstructured data storage mechanism with data often stored in files or (Binary Large Object) blobs.
- **Data warehouse** is structured storage in which data has been normalized to fit a defined data model.
- **Data mart:** A data mart contains data that has been warehoused, analyzed, and made available for specific use such as by a particular business unit.



- **Data mining:** Mining data involves discovering, analyzing, and extracting patterns in data.
- **Online analytic processing (OLAP):** As the name implies, OLAP provides users with analytic processing capabilities for a data source. OLAP consists of consolidation, drill-down, and slice-and-dice functions.
- **Big data:** refers to extremely large and complex datasets that cannot be processed using traditional data processing techniques. These datasets are characterized by their volume, velocity, and variety.
- **Real-time analysis:** Discovery is performed more often and in more diverse ways. Needs to have more fast tools.
- **Agile analytics and Agile business intelligence:** Follow agile methodology of data discovery. Creates a new class of use cases for data discovery.

Structured data

- **Metadata**, or data that describes data, is a critical part of discovery in structured data.
- **Semantics**, or the meaning of data, is described in the schema or data model and can be useful when analyzing the relationships expressed in data.

Unstructured Data: data labels are one approach to dealing with unstructured data. Labels can identify the classification level of a particular file and, by extension, the protections required.

- **Pattern matching**, which compares data to known formats such as credit card numbers that are 16 numeric digits, or unique organization-defined patterns such as user account information.
- **Lexical analysis** attempts to understand the meaning and context of data to discover sensitive information that may not conform to a specific pattern.
- **Hashing** attempts to identify known data such as system files or documents by calculating a hash of files and comparing it to a known set of sensitive file hashes.

Semi-structured data is a type of data that does not fit neatly into traditional relational database tables (structured data) but still has some organizational properties that make it easier to analyze compared to unstructured data. It combines aspects of both structured and unstructured data, often containing tags, markers, or metadata to define and describe the data hierarchy.

Privacy Roles and Responsibilities

Within a cloud environment there are different roles and responsibilities between the cloud provider and the cloud customer regarding data privacy, and those roles differ depending on where the IaaS, PaaS, or SaaS hosting model is employed:

- **Physical environment:** Sole responsibility of the cloud provider for all cloud models
- **Infrastructure:** Sole responsibility of the cloud provider for PaaS and SaaS, with shared responsibility for IaaS between the cloud provider and cloud customer
- **Platform:** Sole responsibility of the cloud provider for SaaS, shared responsibility for PaaS, and responsibility of the cloud customer for IaaS
- **Application:** Shared responsibility for SaaS and sole responsibility of the cloud customer for both IaaS and PaaS
- **Data:** Sole responsibility for the cloud customer for all models
- **Governance:** Sole responsibility of the cloud customer for all models

Implement Data Classification is a way for organizations to provide a uniform set of controls and expectations, as well as a method for speeding up security decision-making. (Data type, Legal constraints, Ownership, Value/criticality)

Mapping: When scanning data sources, discovery tools can use a handful of useful attributes that offer various degrees of efficiency for processing large volumes of data. One efficient approach is the use of metadata.

Labeling: Metadata is a formal part of the data, because it is used in the official data repositories to categorize and organize the data, **labels** are more informal and created by users or processes to show data categories based on subjective and qualitative analysis. (Physical assets, Digital files, Hard-copy materials).

Sensitive Data

Protected health information (PHI) is a term that encompasses data that pertains to an individual and their healthcare histories and specific conditions.

Personal identifiable information (PII) is any data that could be used to identify a specific individual. Examples include driver's license numbers, social security numbers, addresses, full names etc.

Cardholder data (CD) pertains specifically to PII related to an individual who holds a credit or debit card; this includes data such as card numbers, expiration dates, security codes, and any information that ties these to an individual.

Information Rights Management (IRM): IRM adds an extra layer of access controls on top of the data object or document. The ACL determines who can open the document and what they can do with it and provides granularity that flows down to printing, copying, saving, and similar options.

- **Auditing**: Robust auditing of who has viewed information as well as provide proof as to when and where they accessed the data.
- **Expiration:** This gives an organization the ability to set a lifetime for the data.
- **Policy Control:** Very granular and detailed control over how their data is accessed and used, who can copy, save, print, forward, or access data.
- **Protection:** always provides persistent protection that is integrated with the data regardless of its current access state.
- **Support for Applications:** Integration of IRM systems and processes without the organization needing to make major changes to its current operational practices.
- **Interoperability:** Different organizations and users will have a variety of tools, such as email clients and servers, databases, and operating systems. IRM solutions must offer support for users across these different system types.

Data Retention, Deletion, and Archiving Policies

- **Data Retention** – is an organization's established protocol for keeping information for operational or regulatory compliance needs; are to keep important information for future use or reference, to organize information so it can be accessed later, and to dispose of information that is no longer needed.
- **Data Deletion/Destruction** – safe disposal of data once it is no longer needed; failure to do so may result in data breaches or compliance failures
  - **Overwriting:** Zeroization of media
  - **Purge:** The use of specialized tools like overwriting drives with dummy data
  - **Encryption (crypto-shredding):** Crypto-shredding Data is encrypted with a strong encryption engine. The keys used to encrypt the data are then encrypted using a different encryption engine. Then, keys from the second round of encryption are destroyed.
  - **Degaussing:** Strong magnetic field that erases data
  - **Physical destruction:** Destroying media.
  - **Shredding**. You can shred a metal hard drive into powder.
  - **Pulverizing**. Use a hammer and smash drive into pieces, or drill through all the platters.

IaaS Event Sources

- Cloud or network provider perimeter network logs
- Logs from DNS servers
- Virtual machine manager (VMM) logs
- Host OS and hypervisor logs
- API access logs
- Management portal logs
- Packet captures
- Billing records

PaaS Event Sources – the customer has access into applications on the system

- Input validation failures, such as protocol violations, unacceptable encodings, and invalid parameter names and values
- Output validation failures, such as database record set mismatch and invalid data encoding
- Authentication successes and failures

- Authorization (access control) failures
- Session management failures, such as cookie session identification value modification
- Application errors and system events, such as syntax and runtime errors, connectivity problems, performance issues, third-party service error messages, file system errors, file upload virus detection, and configuration changes
- Application and related systems startups and shutdowns, and logging initialization (starting, stopping, or pausing)
- Use of higher-risk functionality, such as network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, and submission of user-generated content, especially file uploads.

SaaS Event Sources – the cloud customer has minimal access into system logs

- Webserver logs
- Application server logs
- Database logs
- Guest OS logs
- Host access logs
- Virtualization platform logs and SaaS portal logs
- Network captures
- Billing records

Identity Attribution Requirements

When:

- Log date and time (international format).
- Event date and time. The event timestamp may be different from the time of logging (for example, server logging where the client application is hosted on a remote device that is only periodically or intermittently online).
- Interaction identifier.

Where:

- Application identifier (for example, name and version).
- Application address (for example, cluster/host name or server IPv4 or IPv6 address and port number, workstation identity, or local device identifier).
- Service (for example, name and protocol).
- Geolocation.
- Window/form/page (for example, entry point URL and HTTP method for a web application or dialog box name).
- Code location (for example, script name or module name).

Who (human or machine user):

- Source address (for example, the users device/machine identifier, the users IP address, cell/RF tower ID, or mobile telephone number).
- User identity, if authenticated or otherwise known (for example, user database tables primary key value, username, or license number).

What:

- Type of event.

- Severity of event (for example, {0=emergency, 1=alert, ..., 7=debug} or {fatal, error, warning, info, debug, trace}).
- Security-relevant event flag (if the logs contain non-security event data too).
- Description.

Open Web Application Security Project (OWASP)

OWASP Top 10	Mitigation Strategies
1. Broken Access Control (A01:2021)	- Implement role-based access controls (RBAC).
	- Enforce least privilege and deny-by-default policies.
	- Test for insecure direct object references (IDOR).
	- Use access control frameworks and tools.
2. Cryptographic Failures (A02:2021)	- Use strong encryption algorithms (e.g., AES-256, RSA-2048).
	- Encrypt data at rest and in transit.
	- Use secure protocols (e.g., TLS 1.3).
	- Ensure proper key management and rotation.
3. Injection (A03:2021)	- Use parameterized queries or prepared statements.
	- Sanitize and validate user input.
	- Escape special characters.
	- Implement web application firewalls (WAFs).
4. Insecure Design (A04:2021)	- Integrate security in the design phase with threat modeling.
	- Use secure design patterns and principles.
	- Conduct security design reviews.
	- Perform regular architectural risk assessments.
5. Security Misconfiguration (A05:2021)	- Disable unused features and services.
	- Enforce secure configurations using automated tools.
	- Regularly update and patch systems.
	- Review configurations against benchmarks (e.g., CIS Benchmarks).
6. Vulnerable and Outdated Components (A06:2021)	- Regularly update software, libraries, and dependencies.
	- Use software composition analysis (SCA) tools.
	- Remove unsupported or unnecessary components.
	- Monitor for known vulnerabilities in third-party components.
7. Identification and Authentication Failures (A07:2021)	- Implement multi-factor authentication (MFA).
	- Use secure session management techniques.
	- Enforce strong password policies.

	- Protect session IDs with secure cookies and token expiration.
8. Software and Data Integrity Failures (A08:2021)	- Secure CI/CD pipelines to prevent unauthorized code deployment.
	- Use digital signatures to verify code integrity.
	- Implement strong access controls for source code repositories.
	- Use tamper-evident techniques for critical data.
9. Security Logging and Monitoring Failures (A09:2021)	- Implement centralized logging and monitoring systems.
	- Use tools to analyze logs for suspicious activities.
	- Enable alerts for abnormal behavior.
	- Regularly test and review incident response plans.
10. Server-Side Request Forgery (SSRF) (A10:2021)	- Validate and sanitize user-provided URLs.
	- Restrict network access for server-side requests.
	- Use allowlists for external requests.
	- Monitor server-side requests for anomalies.

OWASP also lists the following event attributes that should strongly be considered for logging:

Attribute	Description	Purpose
Timestamp	The exact date and time of the event, including time zone.	Provides chronological context and aids in correlating events across logs.
Event Type	The category or type of event (e.g., login, logout, file access, data change).	Helps in filtering, analyzing, and categorizing activities for investigations.
User Identity	Information about the user, such as username, user ID, or session ID.	Identifies the individual or system responsible for the event.
Source IP Address	The IP address from which the event originated.	Detects unauthorized or suspicious access attempts.
Destination IP Address	The IP address of the target system or service.	Tracks communication endpoints and identifies affected systems.
Geolocation	Geographical location associated with the source IP address.	Identifies unusual access patterns, such as access from unexpected regions.
Success or Failure	Indicates whether the event action succeeded or failed.	Highlights anomalies such as repeated failed login attempts that may indicate brute force attacks.
HTTP Request Details	Includes HTTP method (GET, POST, etc.), URL, headers, and body content.	Analyzes requests for malicious payloads or abnormal behaviors.
Event Context	Additional details about the event, such as parameters, input values, or codes.	Provides richer context for investigating the event and troubleshooting.

System Information	Information about the system involved, such as hostname and application name.	Helps in pinpointing affected systems during an investigation.
Authentication Status	Indicates whether the user was authenticated during the event.	Detects unauthorized access attempts and bypass attempts.
Error Messages	Any error messages or codes generated during the event.	Provides insights into potential vulnerabilities or misconfigurations.
Affected Data/Resources	Identifies the data, file, or resource accessed, modified, or deleted.	Tracks the scope of the event and the resources involved.
Application-Specific Details	Additional attributes specific to the application's logic or processes.	Enables tailored logging and monitoring based on unique application functionality.
Response Time	The time taken to process the request or action.	Identifies performance issues or signs of DoS attacks.
Session Details	Includes session ID, creation timestamp, and expiration details.	Tracks session hijacking attempts and unauthorized session reuse.

Storage and Analysis of Data Events

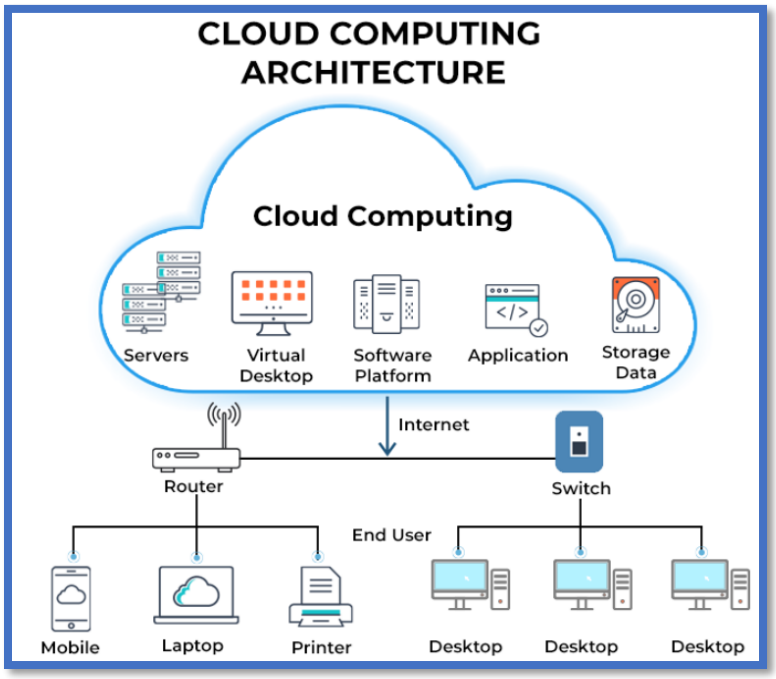
SIEM systems

- Aggregation and Correlation
- Alerting
- Reporting and Compliance
- Dashboards
- Retention and Compliance

Data labeling is the process of assigning labels or tags to raw data (such as images, text, audio, or video) to provide context and meaning for machine learning models. These labels help the model understand the data and make accurate predictions.

Data mapping is the process of identifying and documenting relationships between data elements in different data sources. It involves mapping fields, records, and schemas from one system to another.

Domain 3 - Cloud Platform and Infrastructure Security



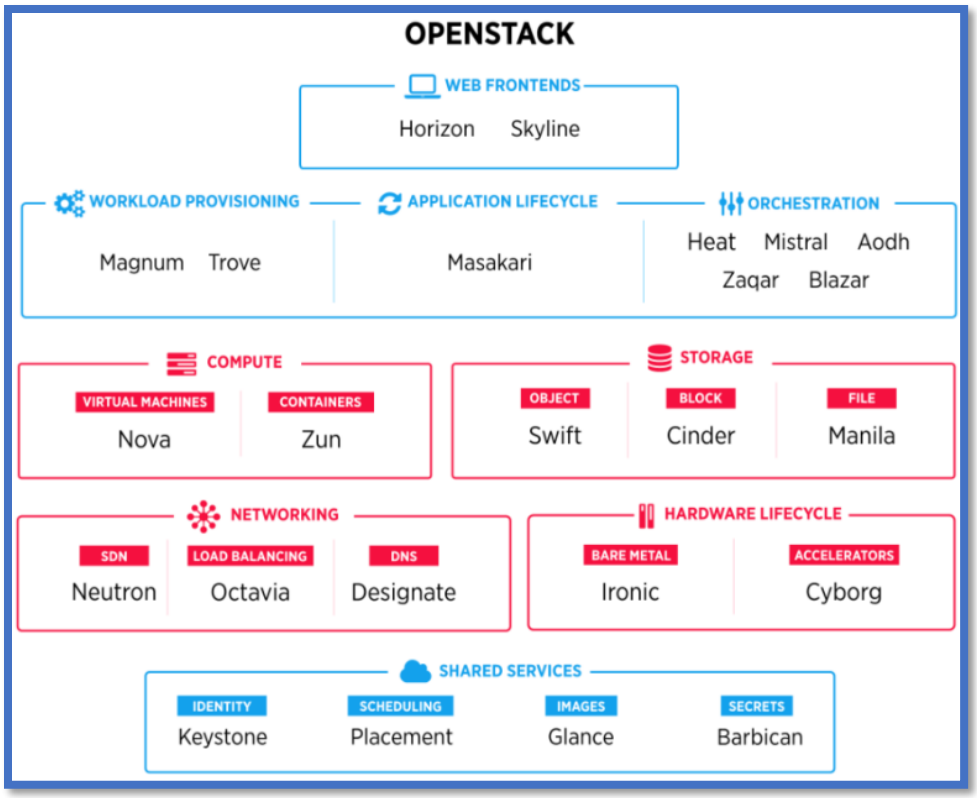
Infrastructure as a Service (IaaS) Customer is responsible for configuring the VMs, virtual network, and guest OS security as if the systems were on-premises. CSP responsible for physical host, physical storage, and physical network.

Software as a Service (SaaS) The customer remains responsible for configuring access to the cloud service for their users, as well as shared responsibility for data recovery. CSP owns physical infrastructure, as well as network and communication.

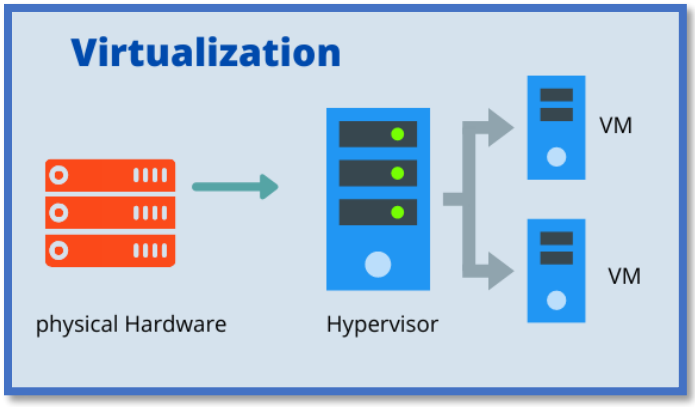
Platform as a Service (PaaS) CSP is responsible for the physical components, the internal network, and the tools provided. Cheaper for customer, but less control.

OpenStack: is a free and open-source infrastructure as a service (IaaS) initiative for creating and managing large pools of storage, processing and networking resources in a data center. Key Components of OpenStack:

- Compute **(Nova)**
- Block Storage **(Cinder)**
- Object Storage **(Swift)**
- Networking **(Neutron)**
- Identity **(Keystone)**
- Dashboard **(Horizon)**
- Image Service **(Glance)**
- Orchestration **(Heat)**
- Telemetry **(Ceilometer)**
- Database Service **(Trove)**
- Bare Metal **(Ironic)**



Virtualization technology is used to host one or more OSs within the memory of a single host computer or to run applications that are not compatible with the host OS. This mechanism allows virtually any OS to operate on any hardware. It also allows multiple OSs to work simultaneously on the same hardware. Common examples include VMware Workstation Pro, VMware vSphere and vSphere Hypervisor, VMware Fusion for Mac, Microsoft Hyper-V Server, Oracle VirtualBox, Citrix Hypervisor, and Parallels Desktop for Mac.

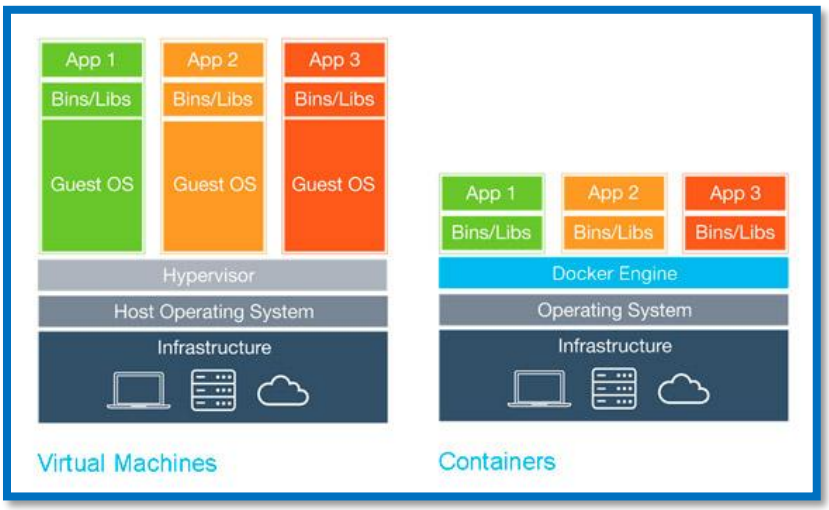


Security recommendations for the hypervisor

- Install all updates to the hypervisor as they are released by the vendor.
- Restrict administrative access to the management interfaces of the hypervisor.
- Capabilities to monitor the security of activity occurring between guest operating systems (VMs).

TIP: The virtual network between the hypervisor and the VM is also a potential attack surface.

Containerization is a form of virtualization where applications run in isolated user spaces, called containers, while using the same shared operating system (OS). One of the benefits of containerization is that a container is essentially a fully packaged and portable computing environment. Everything an application needs to run its binaries, libraries, configuration files, and dependencies is encapsulated and isolated in its container.

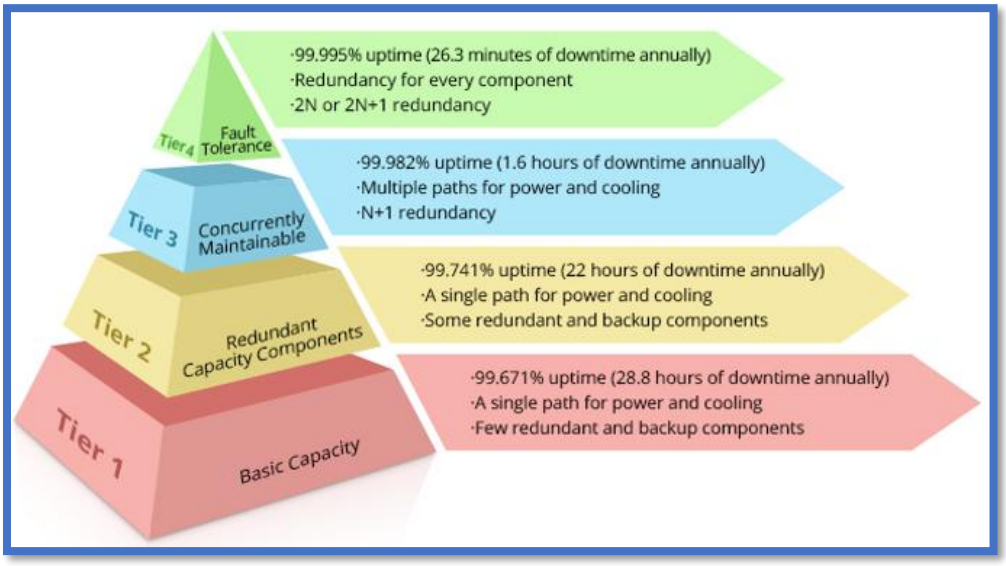


Kubernetes is a container orchestration platform for scheduling and automating the deployment, management, and scaling of containerized applications.

Virtualization and Containerization Attacks

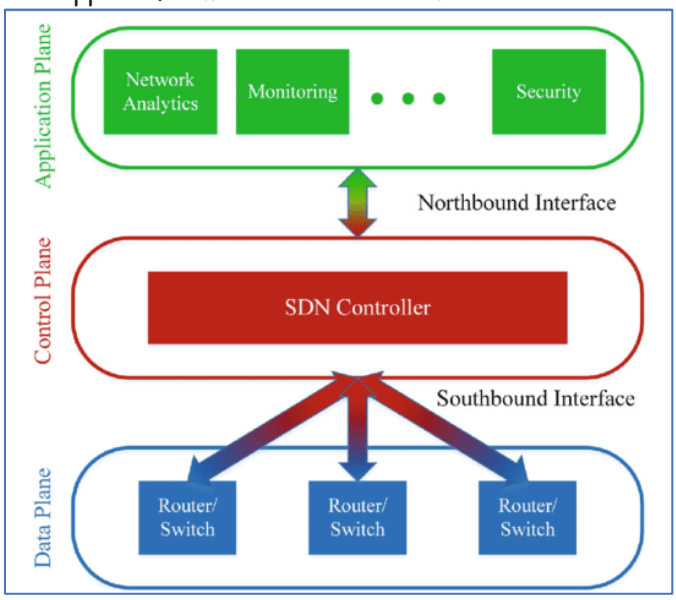
- VM and Container Environment Fingerprinting.
- Guest-to-Guest Virtual Machine (VM) Hopping.
- Guest-to-Host Virtual Machine (VM) Escaping. An exploit that enables a hacker to move from within a virtual machine to the hypervisor, thereby gaining access to the entire computer and all the virtual machines running within it.
- VM Sprawling refers to an excessive and uncontrolled expansion of virtual machines within a virtual infrastructure.
- Virtualization Extension Tampering via Hyper jacking.
- Trusted Platform Module (TPM) Tampering and Abuse.
- Trusted Platform Module (TPM) Message Replay.
- System Management Mode (SMM) and Basic Input-Output System (BIOS) Tampering.
- Input Output Memory Management Unit (IOMMU) enabled Direct Memory
- Access (DMA) Tampering.
- Side Channel Access-Driven and Trace-driven
  - CPU load-based
  - CPU cache-based
- Container-to-Host Escaping.
- Container Image Tampering.

Data center tier standard



Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

- **Management/Application Plane** takes care of the wider network configuration, monitoring and management processes across all layers of the network stack.
- **Control Plane** refers to the network architecture component that defines the traffic routing and network topology.
- **Data Plane** is the network architecture layer that physically handles the traffic based on the configurations supplied from the Control Plane.



Logical Design

- **Tenant Partitioning**: Multitenant models make cloud computing more affordable but create some security and privacy concerns.

- **Access Control:** When creating a logical data center, a primary concern is access. A single point of access makes access control simpler and monitoring better.

Environmental Design

- **Heating, Ventilation, and Air Conditioning:** SOC-2 report should have a section on availability and the controls that provide it.
  - Temperature 64.4–80.6 degrees F (18–27 degrees C)
  - Humidity 40–60 percent relative humidity
- **Multivendor Pathway Connectivity**: use of multiple ISPs or multiple vendors providing connectivity.

Design Resilient

- HA firewalls, active-passive or active-active
- Multi-vendor pathway connectivity
- Web server farm (behind redundant load balancers)
- Database cluster (Windows / Linux cluster feature)

Data Center Design Standards

1. **BICSI (Building Industry Consulting Service International)** certifies complex cabling.
2. **IDCA (International Data Center Authority)** framework for data center design.
3. **NFPA (National Fire Protection Association)** dedicated to eliminating death, injury, property, and economic loss due to fire, electrical hazards, and other related risks.
4. **Uptime Institute** provides data center Tier standard.

System and Communication Protection

- Policy and Procedures
- Separation of System and User Functionality
- Security Function Isolation
- Denial-of-Service Protection
- Boundary Protection: data loss (exfiltration) protection

Audit Mechanisms

- Log Collection
- Packet Capture

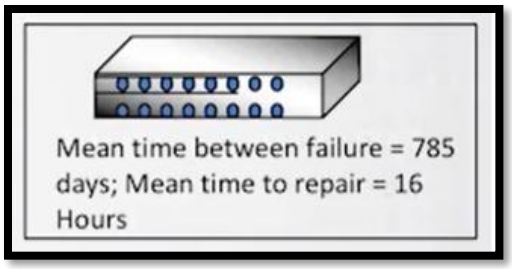
BCP vs DRP

- BCP focuses on the whole business
- DRP focuses more on the technical aspects of recovery

BRP (Business Resumption Plan) the plan to move from the disaster recovery site back to your business environment or back to normal operations.

MTBF (Mean Time Between Failures) a time determination for how long a piece of IT infrastructure will continue to work before it fails.

MTTR (Mean Time to Repair) a time determination for how long it will take to get a piece of hardware/software repaired and back on-line.

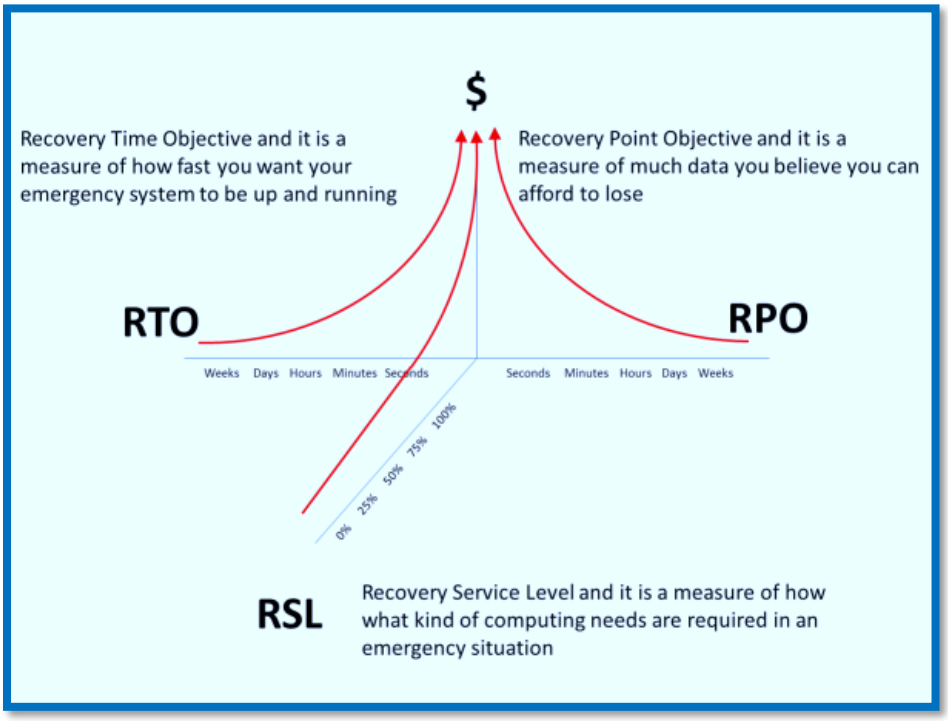


Business impact assessment (BIA) is used to determine which processes are critical and which are not. BIA typically contains a cost-benefit analysis (CBA)and a calculation of the return on investment (ROI).

Cost-benefit analysis lists the benefits of the decision alongside their corresponding costs. CBA can be strictly quantitative: adding the financial benefits and subtracting the associated costs to determine whether a decision will be profitable.

Disaster recovery and business continuity

- ***Recovery Time Objective***. RTO is a time measure of how fast you need each system to be up and running in the event of a disaster or critical failure.
- ***Recovery Point Objective***. RPO is the maximum amount of data your business can afford to lose during an outage, measured in time.
- ***Recovery Service Level***. RSL is a percentage measure (0-100%) of how much computing power is based upon a percentage of the production system that you will need during a disaster.



Disaster Recovery/Business Continuity Strategy

- Define Scope
- Gather Requirements
- Analyze

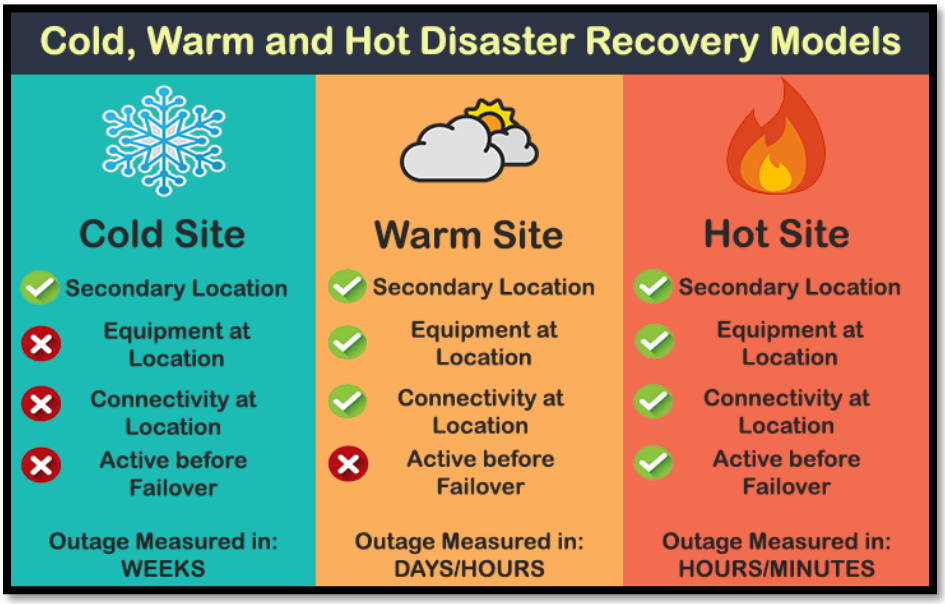
- Assess Risk
  - Load capacity at the BC/DR site
  - Migration of services
  - Legal and contractual issues

BCP/DRP Plan

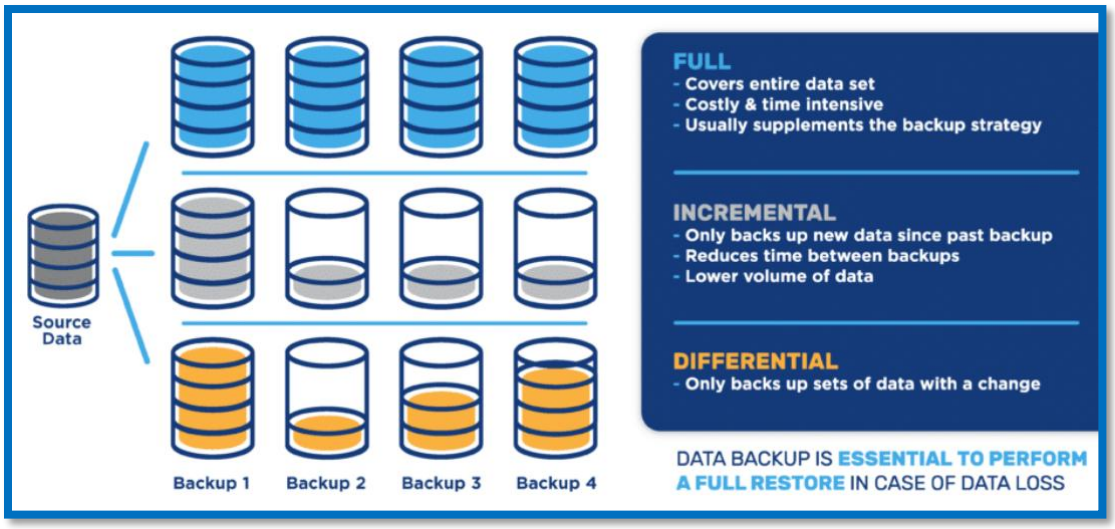
- **Design**: Based on priorities from the business impact analysis (BIA)
- **Implement the Plan**: Implement the plan to protect critical business functions
- **Test the Plan**: Testing ensures both the BCP/DRP function as expected
- **Report and Revise**: BCP/DRP should be revised as necessary based on test results

Disaster recovery test plan:

- **Checklist review / Read Through**: Distributing copies of BCP to stack holders of each critical business unit asking them to review.
- **Tabletop Exercise / Structured Walk-Through Test**: Primary objective is to ensure that critical personnel are aware of BCP and plan accurately reflects the organization's ability to recover from disaster.
- **Simulation Test:** Participants choose a specific scenario and apply BCP to it.
- **Functional Drill / Parallel Test**: People move to an offsite location to see if BCP is properly invoked.
- **Full interruption Test / Full scale Test:** Primary site is stopped and actual BCP is invoked.



Backup Types



Power issues:

- *Fault:* A momentary loss of power
- *Blackout:* A complete loss of power
- *Sag:* Momentary low voltage
- *Brownout:* Prolonged low voltage
- *Spike:* Momentary high voltage
- *Surge:* Prolonged high voltage
- *Transient:* Short duration noise interference

Risk assessment

Exposure factor (EF) represents the percentage of loss that an organization would experience if a specific asset were violated by a realized risk. The EF can also be called the *loss potential*.

Single-loss expectancy (SLE) is the potential loss associated with a single realized threat against a specific asset.

SLE = asset value (AV) * exposure factor (EF)
or more simply: SLE = AV * EF

Annualized rate of occurrence (ARO) is the expected frequency with which a specific threat or risk will occur (that is, become realized) within a single year.

Annualized loss expectancy (ALE) is the possible yearly loss of all instances of a specific realized threat against a specific asset.

ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO)
or
ALE = asset value (AV) * exposure factor (EF) * annualized rate of occurrence (ARO)
or more simply:

ALE = SLE * ARO
or
ALE = AV * EF * ARO

Quantitative Risk Analysis Activity

1. Determine the AV. Let's say that the Web Application has a value of $60,000.
2. Calculate the EF. Let's assume it is 0.85 (85%).
3. Calculate the SLE by multiplying the AV by the EF, which is SLE of $51,000.
4. Determine the ARO. Let's assume it's 0.75 (meaning there's a 75% chance of malicious activity occurring in any given year).
5. Calculate the ALE: $51,000 (SLE) X 0.75 (ARO) = $38,250 (ALE).
6. Compare the ALE to the cost of each of the software solutions you're considering. If the mitigation increases ALE ($38,250), the solution is not a worthwhile investment.

AV = $60,000
EF = 85% (85/100=0.85)
AV x EF = SLE (60,000 x 0.85=51,000)

SLE = $51,000
ARO = 75% (75/100=0.75)
SLE x ARO = ALE (38,250 x 0.75=38,250)
ALE= $38,250

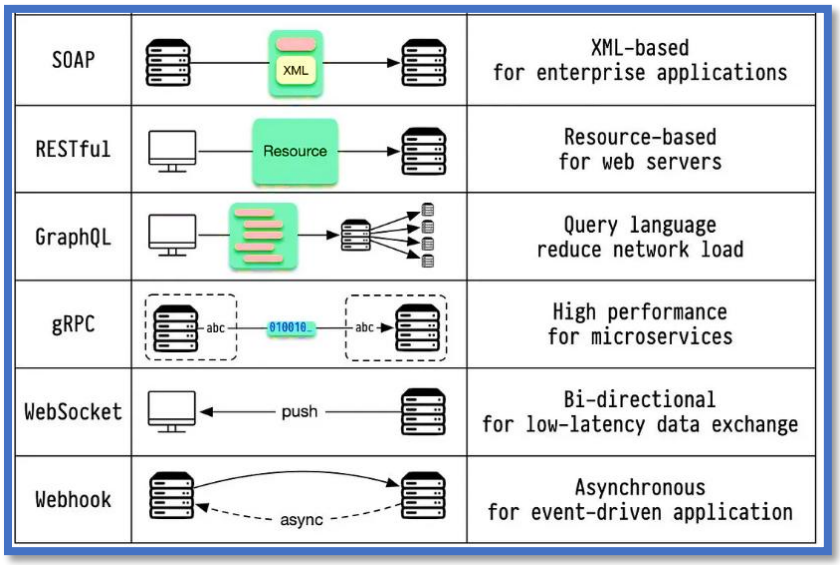
Asset	AV	EF	SLE	ARO	ALE
Web Application	$60,000	85% (0.85)	$51,000	75% (0.75)	$38,250

Domain 4 - Cloud Application Security

Cloud Development Basics

- **Security by design:** This implies that security is part of every step in the process.
- **Shared security responsibility:** The idea is that security is the responsibility of everyone.
- **Security as a business objective:** Security is not something in addition to what we do. Instead, Security is part of all business objectives.

Types of API



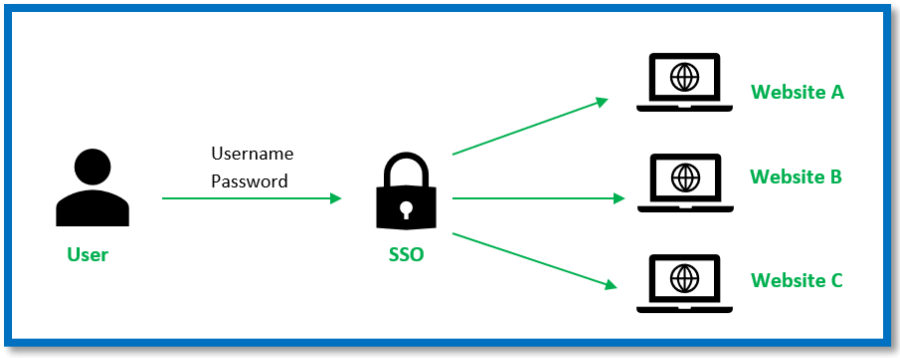
Aspect	SOAP API	REST API
Protocol	Strict protocol that defines rules for messaging.	Architectural style
Data Format	XML only	JSON, XML, HTML, plain text
Transport	HTTP, SMTP, FTP, etc.	HTTP/HTTPS only
Speed	Slower due to XML overhead	Faster due to lightweight JSON
Complexity	More complex and rigid	Simpler and flexible
Security	WS-Security (built-in)	HTTPS-based security
Statefulness	Stateful or stateless	Stateless
Performance	Higher overhead	More efficient and scalable
Best Use Case	Enterprise systems, banking	Web services, mobile applications, Microservices Architecture, Cloud and IoT

APIs Threats

- Injection attacks
- Denial-of-service attacks
- Poorly secured API servers or services
- On-path attacks

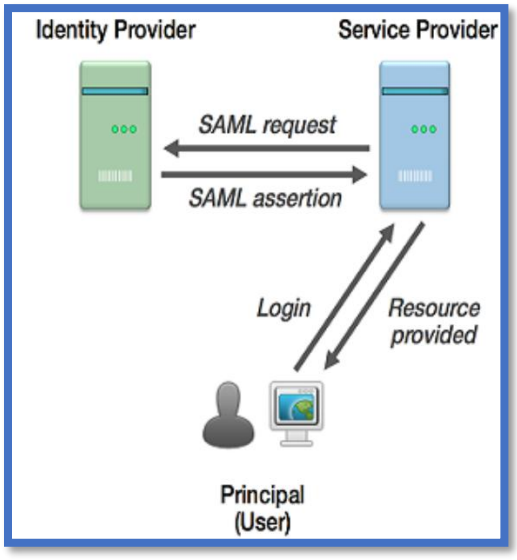
- Credential attacks, including stolen credentials, accidental API key exposures, and brute force attacks
- Poor API key generation techniques

Single sign-on (SSO) is a system that allows users to access multiple applications and services with just one set of login credentials.



Security Assertion Markup Language (SAML) is an open XML-based standard commonly used to exchange authentication and authorization (AA) information between federated organizations. It provides SSO capabilities for browser access.

- **Principal or User Agent**: End User
- **Service Provider (SP)** providing the service requested by end user.
- **Identity Provider (IdP)** This is a third party that holds the user authentication and authorization information.

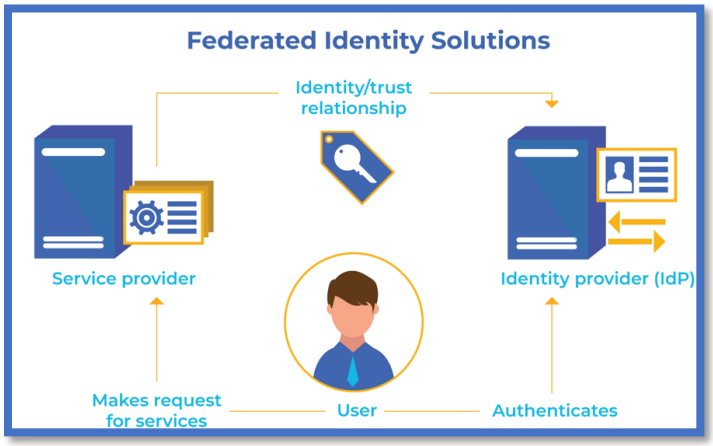


EXtensible Access Control Markup Language (XACML) is a standard for defining attribute-based access controls/authorizations. It is a policy language for defining access controls at a Policy Decision Point and then passing them to a Policy Enforcement Point.

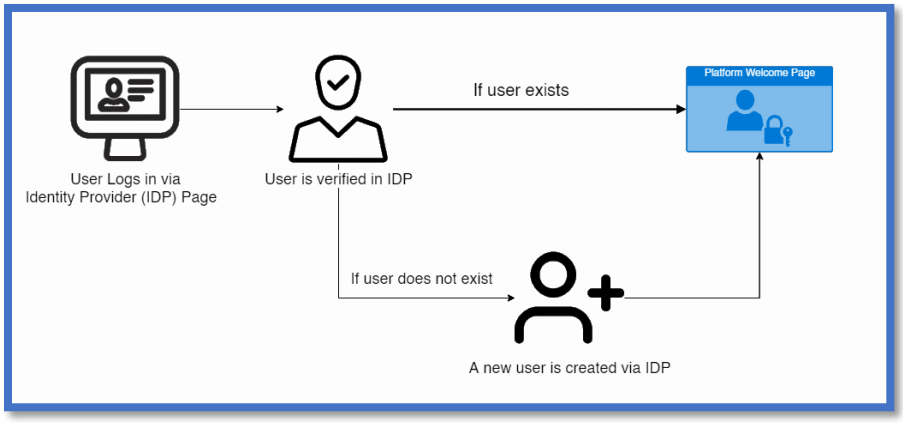
System for Cross-domain Identity Management (SCIM) is a standard for exchanging identity information between domains. It can be used for provisioning and deprovisioning accounts in external systems and for exchanging attribute information.

Cloud-based federation typically uses a third-party service to share federated identities.

As an example, many corporate online training websites use federated SSO systems. When the organization coordinates with the online training company for employee access, they also coordinate the federated access details.



Just-in-Time (JIT) Some federated identity solutions support *just-in-time (JIT)* provisioning. These solutions automatically create the relationship between two entities so that new users can access resources. A JIT solution creates the connection without any administrator intervention.



Secure SDLC

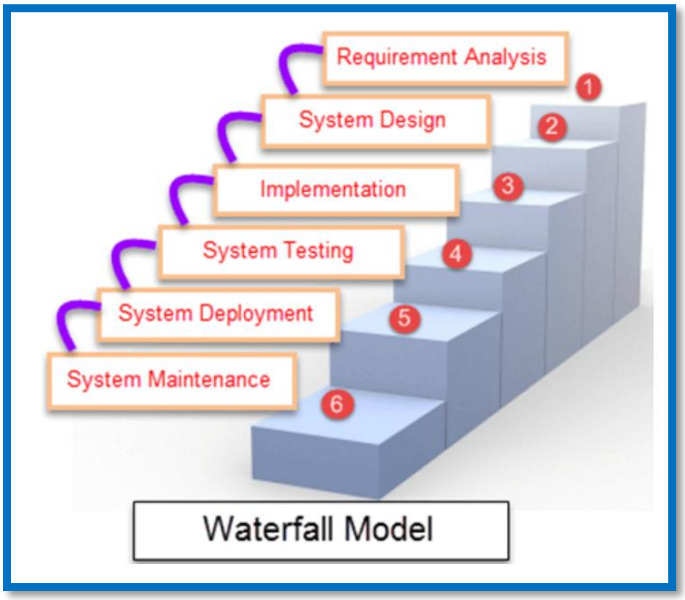
- Requirements
  - Identify functional and security requirements for the software.
  - Perform a risk assessment to understand potential threats.
- Design
  - Develop secure architecture and system design.
  - Conduct threat modeling to identify and address potential vulnerabilities.
  - Plan for secure authentication, encryption, and access control mechanisms.
- Development
  - Use secure coding standards (e.g., OWASP, CERT).
  - Perform code reviews to identify vulnerabilities early.
  - Employ static application security testing (SAST) tools to catch issues during coding.
- Testing
  - Conduct dynamic application security testing (DAST) to identify runtime vulnerabilities.
  - Perform penetration testing to simulate real-world attacks.

- Validate security features like access control, encryption, and input validation.

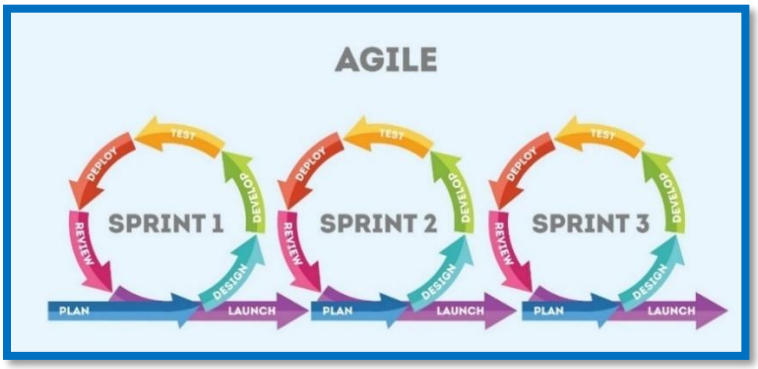
➡ Deployment
- Ensure the production environment is secure (e.g., server hardening, secure configurations).
- Use secure CI/CD pipelines to prevent injecting vulnerabilities.
- Conduct final security checks before releasing the software.

➡ Operations and Maintenance
- Keep the software updated with security patches.
- Monitor the software for new vulnerabilities and security incidents.
- Monitor for new threats and fix them as needed.

Waterfall: The traditional waterfall method of development is built upon phases of a project. Each phase is contained, and development does not move on to the next phase until the current phase has been fully developed, tested, validated, approved, and implemented. There is no way to return to previously completed phases.



Agile development works by breaking development into a series of "sprints" that can be done and implemented quickly and in an iterative process. As each component is completed, it can be deployed and closed out to focus on the next process.



Cloud-Specific Risks

1. Data breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

Threat Modeling

- Define security requirements
- Create application overview
- Identify threats
- Mitigate threats
- Validate threat mitigation

STRIDE

Threat	Definition	Property	Example
Spoofing	Pretend to be someone else.	Authentication	Hack victim's email and use to send messages in name of the victim.
Tampering	Change data or code.	Integrity	Software executive file is tampered by hackers.
Repudiation	Claiming not to do a particular action.	Non-repudiation	"I have not sent an email to Alice".
Information Disclosure	Leakage of sensitive information.	Confidentiality	Credit card information available on the internet.
Denial of Service	Non-availability of service	Availability	Web application not responding to user requests.
Elevation of privilege	Able to perform unauthorized action	Authorization	Normal user able to delete admin account

Visual, Agile, and Simple Threat (VAST) is a threat modeling concept that integrates threat and risk management into an Agile programming environment on a scalable basis.

DREAD

- **Damage How** severe is the damage likely to be if the threat is realized?
- **Reproducibility** How complicated is it for attackers to reproduce the exploit?
- **Exploitability** How hard is it to perform the attack?
- **Affected Users** How many users are likely to be affected by the attack (as a percentage)?
- **Discoverability** How hard is it for an attacker to discover the weakness?

Architecture, Threats, Attack Surfaces, and Mitigations (ATASM) is a threat-modeling approach that focuses on the structural basis of a system. It is composed of the following components:

- **Architecture** The systems architecture is broken into both physical and logical components for analysis.
- **Threats** combine any type of potential attacks a system is likely to face based on their exposure, design, and purpose.
- **Attack Surfaces** Any inputs and outputs of a system are potential attack surfaces.
- **Mitigations** Defines where in the system design and architecture mitigations may be applied.

PASTA (Process for Attack Simulation and Threat Analysis) focus on developing countermeasure based on asset value.

- Stage I: Definition of the Objectives (DO) for the Analysis of Risks
- Stage II: Definition of the Technical Scope (DTS)
- Stage III: Application Decomposition and Analysis (ADA)
- Stage IV: Threat Analysis (TA)
- Stage V: Weakness and Vulnerability Analysis (WVA)
- Stage VI: Attack Modeling & Simulation (AMS)
- Stage VII: Risk Analysis & Management (RAM)

Software Assurance Forum for Excellence in Code (SAFECode) is a global, nonprofit organization dedicated to enhancing software security. It serves as a collaborative platform where business leaders and technical experts share insights and develop effective software security programs.

Application Security Verification Standard (ASVS) is a globally recognized standard for assessing the security posture of web applications. It provides a comprehensive set of security requirements and testing procedures to help organizations build and maintain secure web applications.

- **Level 1 (Basic Verification):** This level is for applications with low security requirements, such as public websites with limited access control needs. It includes basic security requirements such as proper authentication, session management, and access control.
- **Level 2 (Standard Verification):** This level targets applications that handle sensitive data and require higher security controls. It includes more detailed controls for authorization, data protection, and application logic.
- **Level 3 (Advanced Verification):** This level is designed for high-security applications (e.g., financial or government applications). It includes the most comprehensive set of security controls and requires a thorough, detailed examination of an application's architecture, source code, and behavior.

Functional Testing

- ***Integration testing*** that validates whether components work together.
- ***Regression testing*** is a software testing practice that ensures an application still functions as expected after any code changes, updates, or improvements.
- ***Unit Testing***: Testing individual components or functions of the application.
- ***System Testing***: Testing the entire application as a whole.
- ***Smoke Testing***: Preliminary testing to ensure critical functionalities are working before detailed testing begins.
- ***User acceptance testing*** which tests how users interact with and operate the software.

Nonfunctional testing focuses on testing the quality of the software, looking for things like the stability of the software or its performance. Load testing, stress testing, and similar testing techniques are all examples of nonfunctional testing.

- ***Performance Testing:*** Measures responsiveness, stability, and throughput under different workloads.
- ***Load Testing:*** Examines the system's behavior under expected user loads.
- ***Stress Testing:*** Tests the system's robustness by pushing it beyond normal operational limits.
- ***Scalability Testing:*** Determines how well the system scales up or down in response to varying demands.
- ***Security Testing:*** Identifies vulnerabilities and ensures data protection.
- ***Usability Testing:*** Evaluates how easy and intuitive the system is for end-users.
- ***Reliability Testing:*** Assesses the system's ability to perform consistently over time.
- ***Availability Testing:*** Ensures the system is accessible as per the agreed-upon uptime.
- ***Compliance Testing:*** Verifies adherence to legal, regulatory, and industry standards.
- ***Compatibility Testing:*** Confirms the software works across various devices, operating systems, browsers, or networks.
- ***Disaster Recovery Testing:*** Validates the system's ability to recover from crashes or failures.
- ***Localization and Internationalization Testing:*** Ensures the application is adapted for different languages, regions, and cultures.

Security Testing Methodologies

- **White-box testing:** Tests the internal structures of the software. This requires access to the software. Static application security testing (SAST) is a form of white-box testing.
- **Gray-box testing:** Tests a system with limited information about the application. The tester does not have access to the code but will have knowledge of things such as algorithms and architectures. It is primarily used in integration and penetration testing.
- **Black-box testing:** Tests a system with no knowledge of the code, algorithms, or architecture. Dynamic Application Security Testing (DAST) is a form of black-box testing.

Static application security testing (SAST) is a type of application security testing that analyzes source code, bytecode, or binary code for vulnerabilities and security weaknesses. Unlike dynamic testing, SAST examines the code without executing the application, making it a white box testing method. Static analysis usually involves the use of automated tools designed to detect common software flaws, such as buffer overflows and it requires source code. SAST is for finding vulnerabilities in code during development.

Dynamic application security testing (DAST) is a black box testing method that analyzes an application's behavior during runtime to identify security vulnerabilities. DAST interacts with the running application to simulate attacks and uncover issues that only manifest during execution. One common example of dynamic software testing is the use of web application scanning tools to detect the presence of cross-site scripting, SQL injection, or other flaws in web applications. Dynamic testing may include the use of ***synthetic transactions*** to verify system performance. DAST is for testing vulnerabilities in a live application.

Interactive Application Security Testing (IAST) is a modern approach to application security testing that combines features of Static Application Security Testing (SAST) and Dynamic

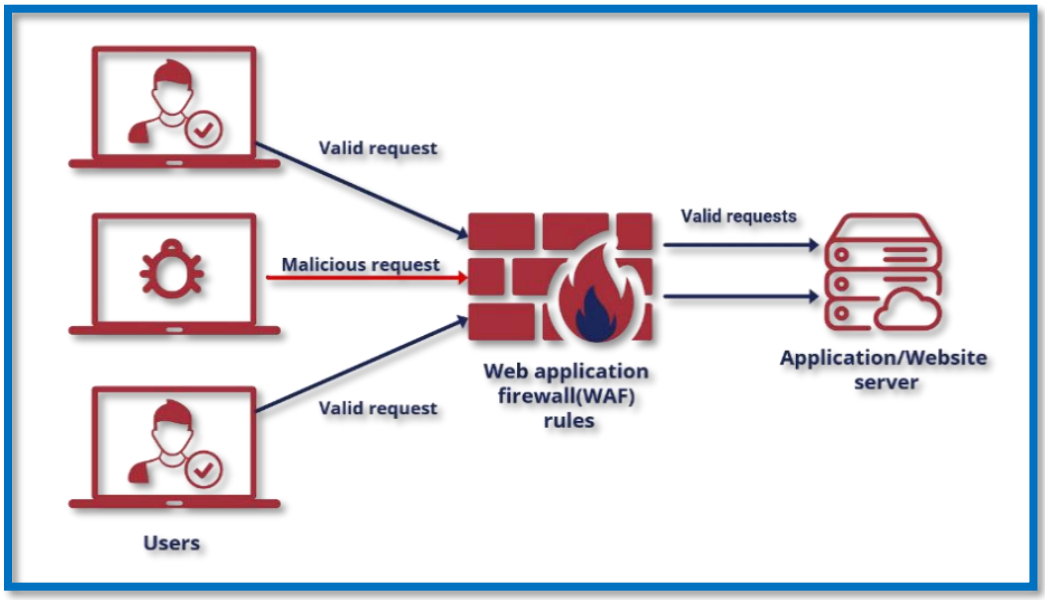
Application Security Testing (DAST). IAST operates by analyzing applications in real-time as they are running, providing deeper insights into vulnerabilities within the application's code, configuration, and runtime environment. IAST agents are usually deployed on the application servers, and when DAST scanner performs its work by reporting a vulnerability the IAST agent that is deployed will now return a line number of the issue from the source code.

RASP (Runtime application self-protection) is a powerful technology that intercepts all calls from the app to a system, making sure they're secure. It validates data requests directly inside the app. Two primary RASP capabilities are:

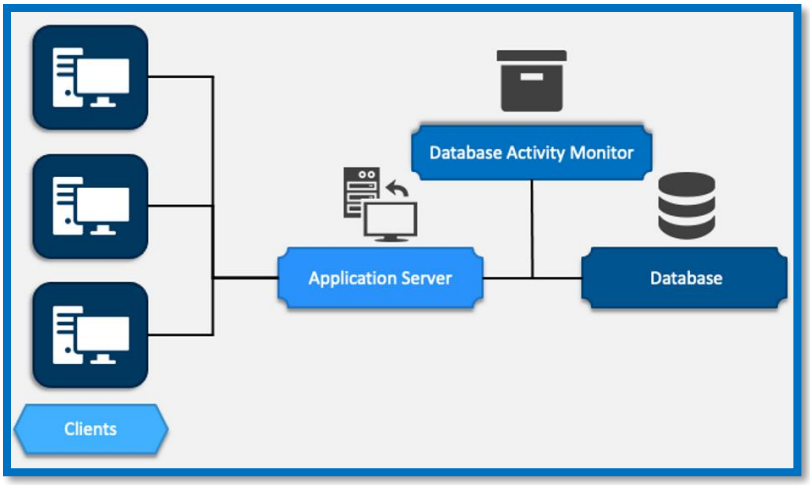
1. Application protection: Accurately stopping application vulnerabilities from being exploited without disrupting legitimate application use.
2. Application threat intelligence: Giving security teams visibility into who is attacking, the techniques they are using, and the applications they are targeting down to the code level.

Abuse Case Testing is a security-focused testing technique designed to identify and mitigate potential vulnerabilities by simulating malicious actions or misuse scenarios. Instead of testing how a system behaves under normal conditions (use cases), abuse case testing evaluates how it responds to intentional misuse or adversarial attacks.

Web application firewall (WAF) protects HTTP/HTTPS applications from common attacks. Usually, a WAF protects an Internet-facing application. WAF helps protect against SQL injection, cross-site scripting (XSS) and cross-site forgery, and other attacks. WAF is also called reverse proxy.

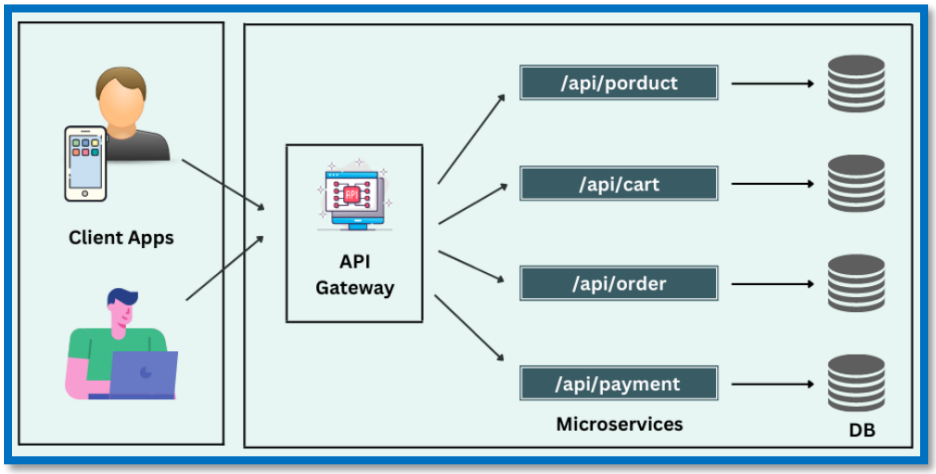


Database activity monitoring (DAM) refers to a set of tools that supports the identification and reporting of fraudulent or suspicious behavior in the databases used by your application services.



Extensible Markup Language Firewalls: XML firewalls work at the application layer to protect XML-based applications and APIs over HTTP, HTTPS, and other messaging protocols.

API gateway is a type of service that sits between a client and a collection of backend services. When a client makes a request to your back-end services, the API gateway routes the request to the service and returns the response to the client. The API gateway can perform other tasks, such as authentication, rate limiting, and monitoring. By offloading these tasks from your back-end services, the API gateway can improve the performance of the system.



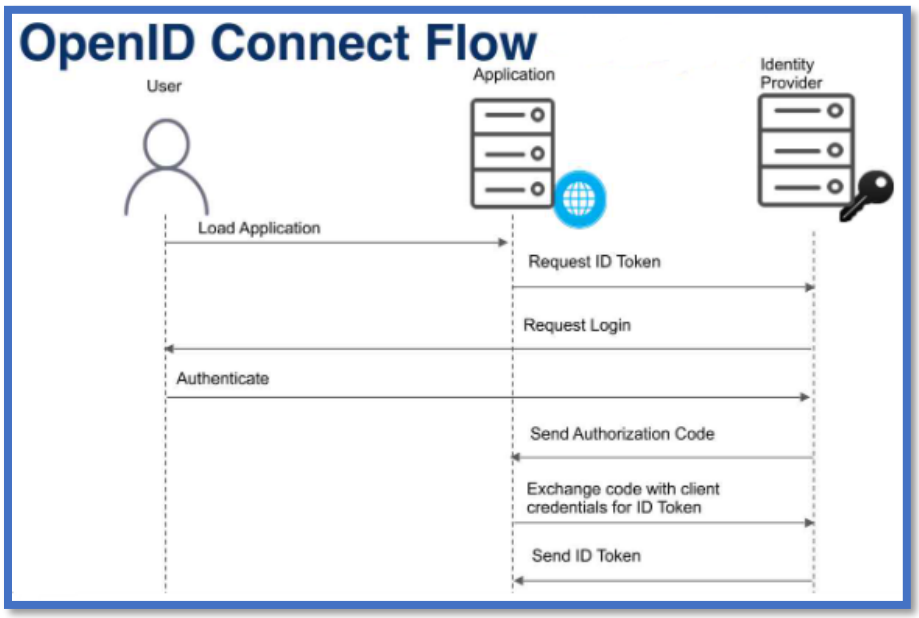
Identity Provider (IdP) is a service or system that manages user identities and authentication, enabling users to access various applications, systems, and services without needing separate credentials for each.

Federated identity is related to single sign-on (SSO). Federated identity allows authorized users to access multiple applications and domains using a single set of credentials. It links a user's identity across multiple identity management systems so they can access different applications securely and efficiently.

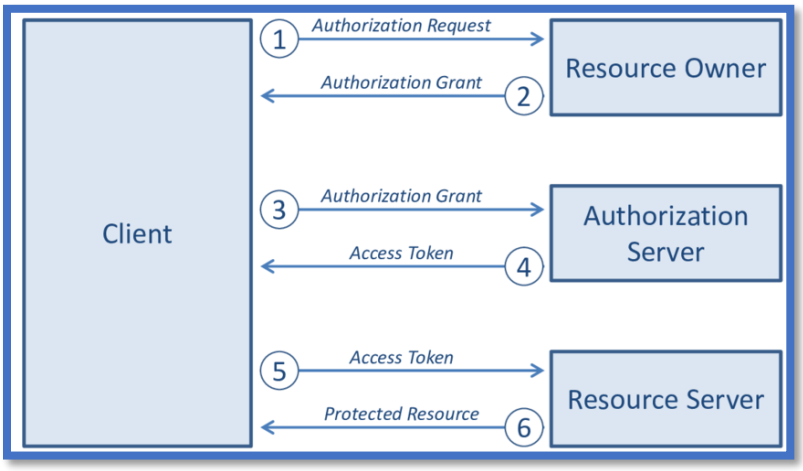
WS-Federation (Web Services Federation) is a standard protocol that enables secure sharing of identities between organizations or systems (called federation). It allows users to authenticate

once in one domain and access resources or applications in another domain without needing to log in again (single sign-on or SSO).

Open ID Connect: an identity authentication protocol used to enable two unrelated applications to share user profile information without compromising user credentials, protocol based on OAuth 2.0.



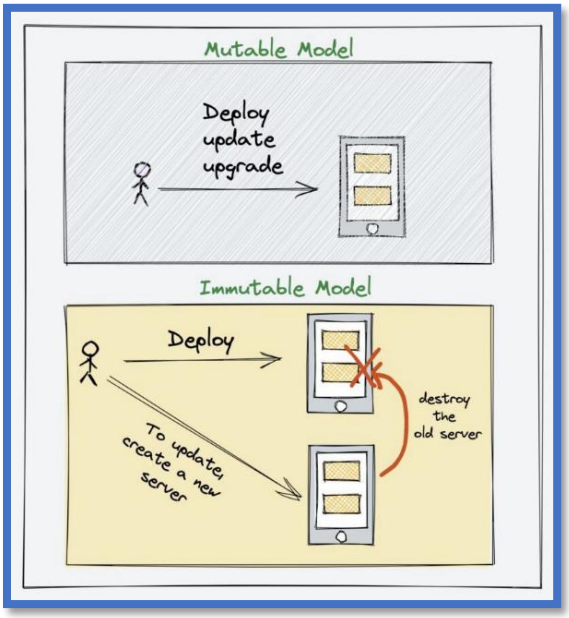
OAuth: OAuth 2.0 is an open standard for authorization that allows secure access to resources on behalf of a user. It enables third-party applications to gain limited access to an HTTP service (such as a website, API, or mobile app) without exposing user credentials. OAuth 2.0 is widely used in scenarios such as enabling social logins, accessing APIs, and managing authorization across multiple systems.



Shibboleth Standard: User authenticates with their organization's credentials and the organization (Identity Provider) passes information to service providers.

Mutable infrastructure refers to a server environment that can be updated, modified, or tuned even after deployment.

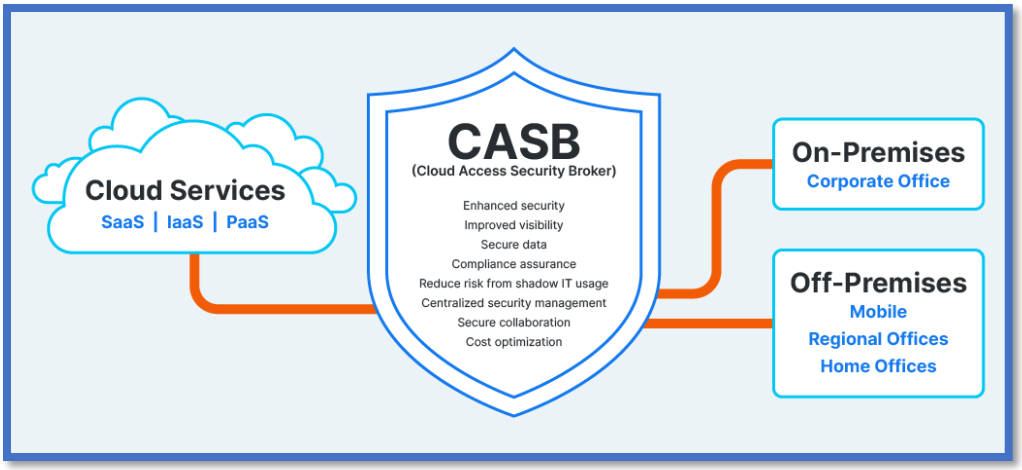
Immutable infrastructure is a concept where you don't make any changes to the server after you deploy it. Meaning the server gets deployed with preconfigured configurations, utilities, and applications. The moment the server comes up, the application starts running. If you want to make any changes, the existing services should be destroyed and replaced with a new one. A change could be patching, application upgrade, server configuration change, etc.



Cloud access security broker (CASB) is software placed logically between users and cloud-based resources. CASB would typically include authentication and authorization controls and ensure only authorized users can access the cloud resources. CASB solutions can also be effective at detecting *shadow IT*. CASBs offer a range of security capabilities, including:

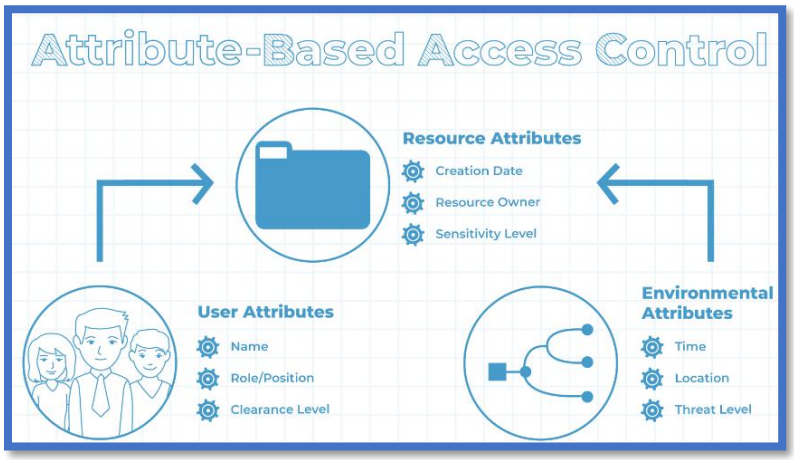
- Access controls: CASBs can be used to enforce access controls and ensure that only authorized users and devices have access to cloud-based resources.
- Data security: CASBs can be used to protect data that is stored on the cloud, including measures such as data encryption and data loss prevention (DLP).
- Compliance: CASBs can help organizations meet regulatory and compliance requirements when it comes to storing and processing data in the cloud.
- Threat detection and response: CASBs can be used to monitor cloud-based resources for potential threats and vulnerabilities, and to respond to incidents as needed.

CASBs are often used as part of a larger cloud security strategy, along with other security solutions such as **Cloud Security Posture Management (CSPM)** and **Cloud Workload Protection Platforms (CWPP)**.

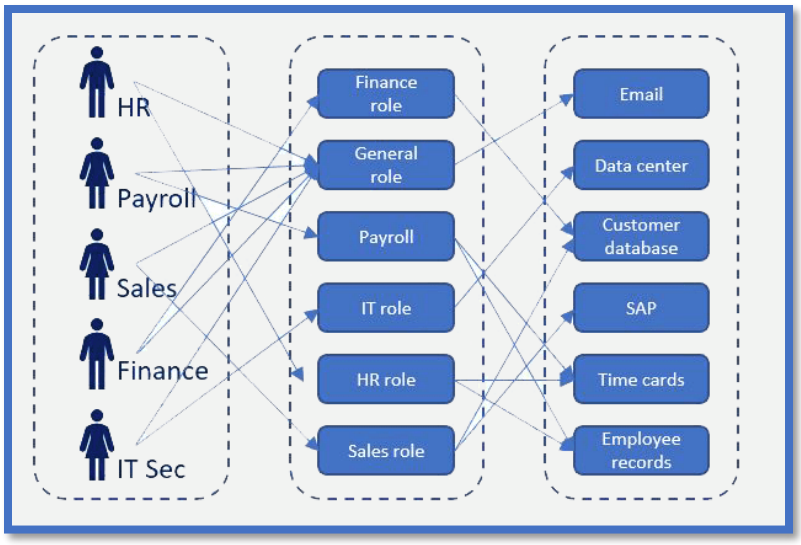


Data loss prevention (DLP) is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

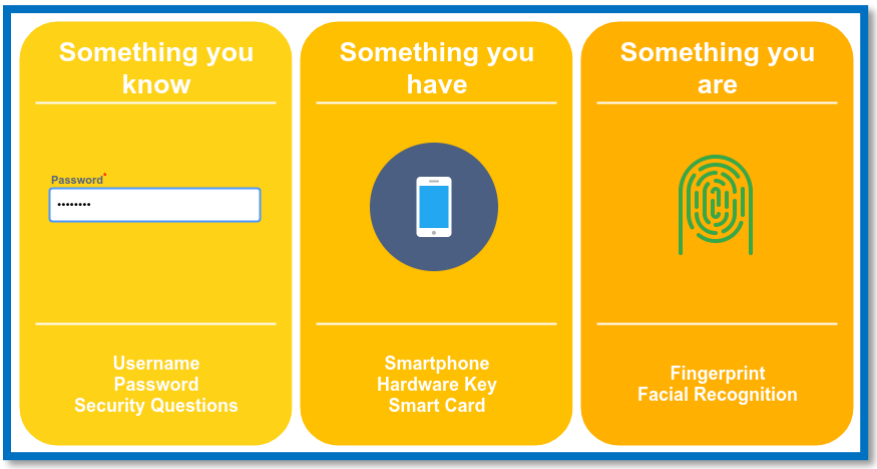
Attribute-Based Access Control (ABAC) model is its use of rules that can include multiple attributes. This allows it to be much more flexible than a rule-based access control model that applies the rules to all subjects equally. Many software-defined networks (SDNs) use the ABAC model. Additionally, ABAC allows administrators to create rules within a policy using plain language statements such as "Allow Managers to access the WAN using a mobile device."



Role-Based Access Control A key characteristic of the Role-Based Access Control (RBAC) model is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. These roles are typically identified by job functions. If a user account is in a role, the user has all the privileges assigned to the role.



Multi Factor Authentication



- **Something you know (Type I):** This includes answers to security questions and identification of previously selected photos/pictures, PINs, and passwords.
- **Something you have (Type II):** Examples include a hardware token, smartphone, or a card, such as a debit card or smart card.
- **Something you are (TYPE III):** This category generally refers to biometrics. This is generally fingerprint, facial recognition, or iris scans. Of the three, these are the most challenging to do reliably and at a reasonable cost.

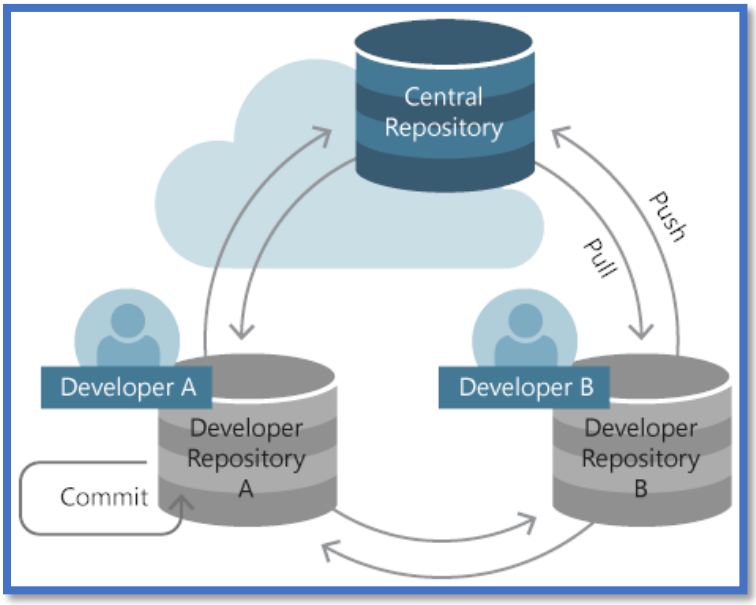
There are multiple options for MFA, including:

- **Hard tokens** are physical devices that generate one-time passwords for human entry or need to be plugged into a reader. These are the best option when the highest level of security is required.
- **Soft tokens** work similarly to hard tokens but are software applications that run on a phone or computer. Soft tokens are also an excellent option but could be compromised if the user's device is compromised, and this risk needs to be considered in any threat model.
- **Out-of-band Passwords** are text or other messages sent to a user's phone (usually) and are then entered like any other one-time password generated by a token.

- **Biometrics** For cloud services, biometric is a local protection that doesn't send biometric information to the cloud provider and is instead an attribute that can be sent to the provider. As such the security and ownership of the local device needs to be considered.

Time-of-Check-to-Time-of-Use (TOC/TOU) a timing vulnerability that occurs when a program checks access permission too far in advance of a resource request. It's also called *race condition*.

Code repositories are centralized locations for the storage and management of application source code. The main purpose of a code repository is to store the source files used in software development in a centralized location that allows for secure storage and the coordination of changes among multiple developers. Code repositories also perform version control, allowing the tracking of changes and the rollback of code to earlier versions when required.



Software bill of materials (SBOM) lists all the components in an application or service, including open source or proprietary code libraries.

Software Composition Analysis (SCA) is used to track the components of a software package or application that is of special concern for apps built with open-source software components because open-source components often involve reusable code libraries.

Secrets management is the practice of securely storing, accessing, and distributing sensitive information, such as passwords, API keys, tokens, encryption keys, and other confidential data used in software applications, infrastructure, and services.

Domain 5- Cloud Security Operations

BIOS as with any physical hardware, virtualization hosts and trusted platform modules (TPMs) have BIOS settings that govern specific hardware configurations and security technologies to prevent access to them for the purpose of manipulation.

Hardware Security Module (HSM) is a physical device typically a plug-in card or an external device that attaches to a physical computer used to perform encryption and decryption for digital signatures, authentication operations, and other services where cryptography is necessary. HSMs are certified to FIPS-140.

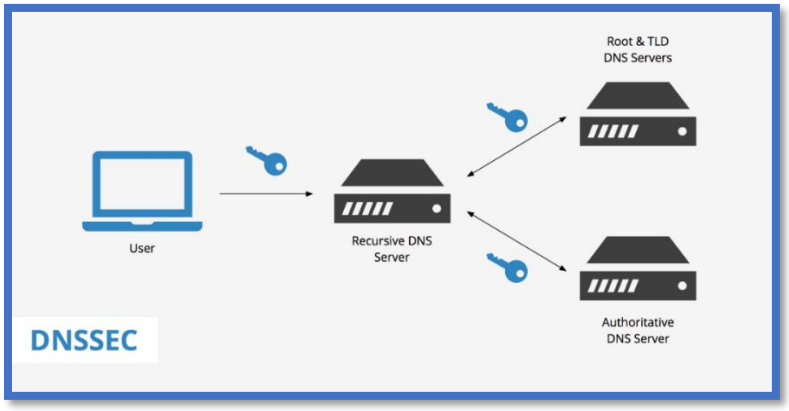
Trusted Platform Module (TPM) is a secure and dedicated microcontroller on a computing system used to perform cryptographic operations on keys. The chip contains a hardware-secured random number generator, functions for generating cryptographic keys, and a variety of other functions for attesting to the security and authenticity of security keys. TPM is provided in ISO/IEC 11889.

Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP that operates at layer 3. This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public internet connections. iSCSI is often viewed as a low-cost alternative to Fiber Channel. iSCSI supports variety of authentication protocols, such as Kerberos and CHAP, for securing communications and confidentiality within networks.

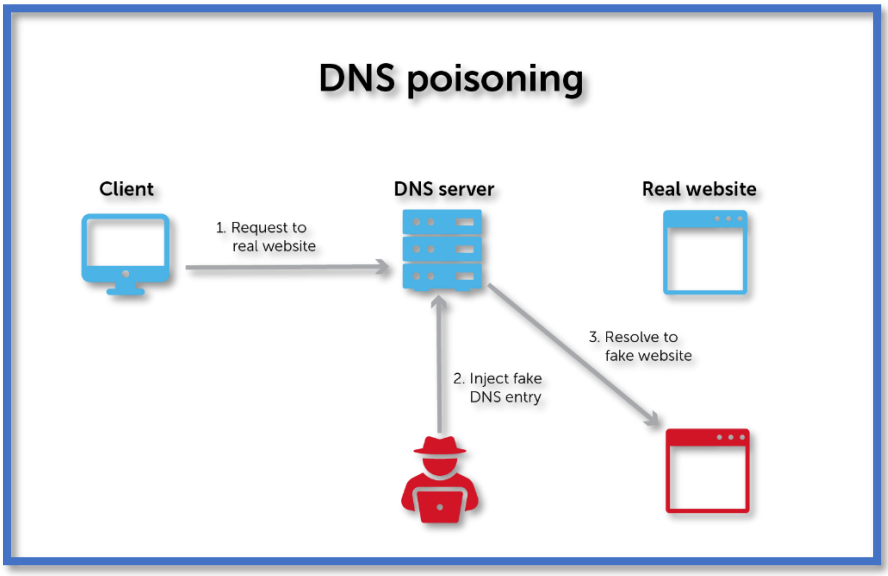
Access Controls for Local and Remote Access

- Secure KVM
- Console-Based Access Mechanisms
- Remote Desktop Protocol
- SSH
- Jump box
- Virtual Client

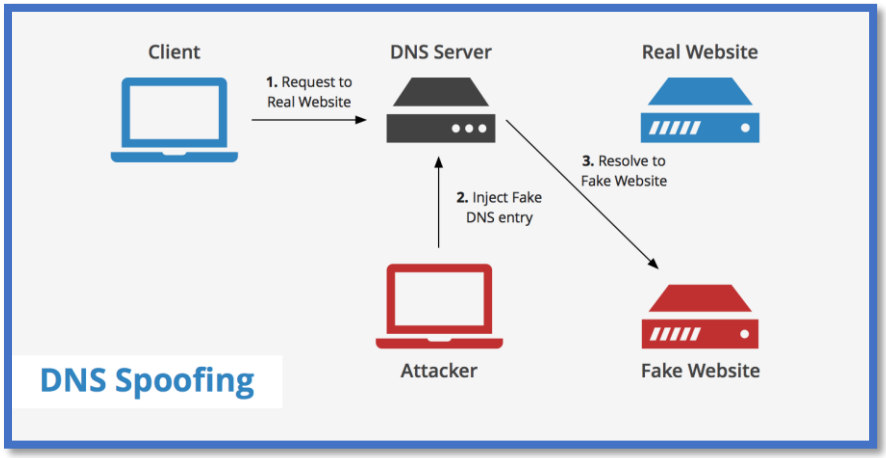
DNSSEC (Domain Name System Security Extensions) is a suite of extensions to the Domain Name System (DNS) designed to add a layer of security. It ensures the authenticity and integrity of DNS data by using cryptographic signatures, helping to protect against DNS spoofing and man-in-the-middle attacks. DNSSEC relies on digital signatures and allows a client lookup to validate a DNS record back to its authoritative source, a process known as *zone signing*.



DNS Cache poisoning is an attack where a malicious user updates a DNS record to point an FQDN to an incorrect IP address.

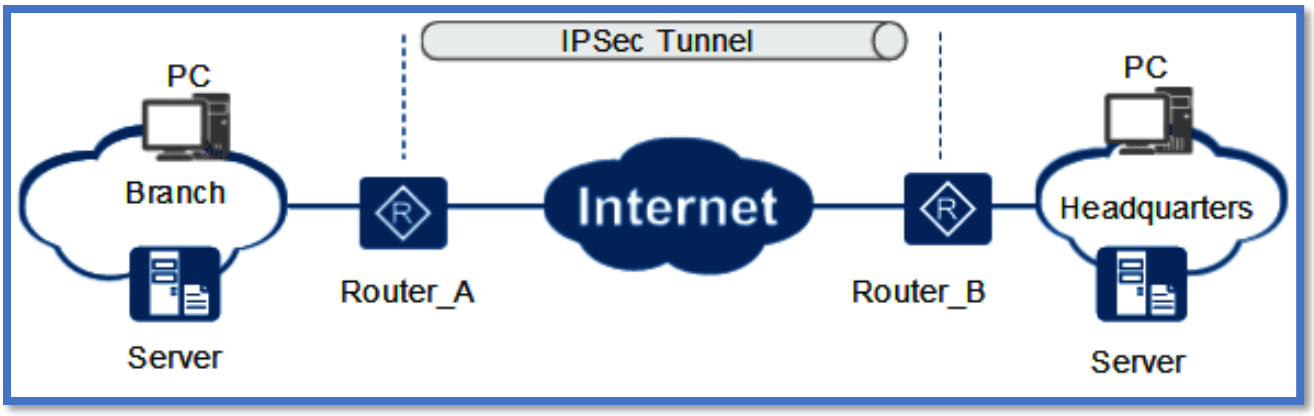


DNS spoofing is another attack against DNS. In this case, an attacker spoofs a DNS service on a network with the goal of resolving a user's requested FQDN to an attacker controlled IP address.

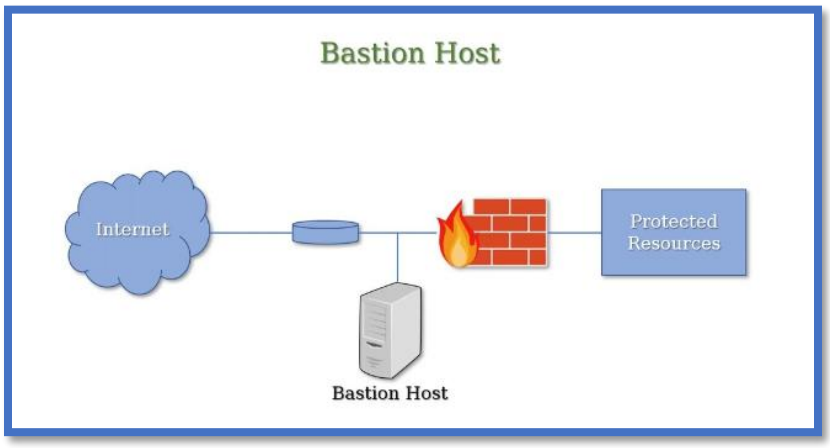


IPSec is a protocol for encrypting and authenticating packets during transmission between two parties, which can be a pair of servers, a pair of network devices, or network devices and servers. The protocol will perform both authentication and negotiation of security policies between the two parties at the start of the connection and then maintain them throughout its use. IPSec and other protocols such as TLS are that IPSec operates at the Internet network layer rather than the application layer, allowing for complete end-to-end encryption of all communications and traffic.

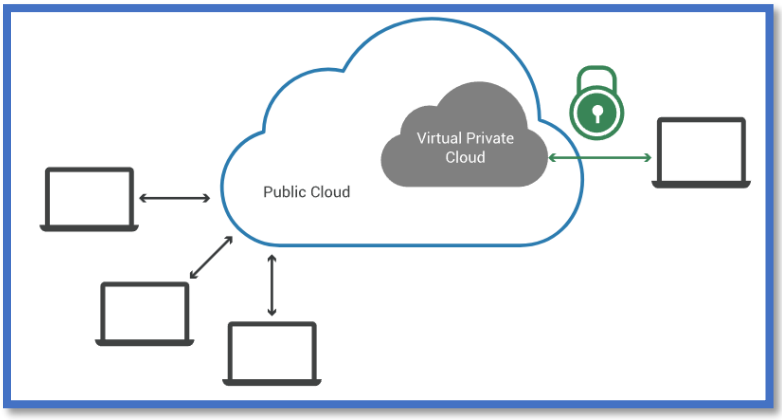
- ***Authentication Header (AH)*** provides assurances of message integrity and nonrepudiation but no confidentiality. AH also provides authentication and access control and prevents replay attacks. AH adds a keyed hash of the message to the packet. This hash is referred to as the Integrity Check Value (ICV). In the ICV computation.
- ***Encapsulating Security Payload (ESP)*** provides confidentiality and integrity of packet contents. It provides encryption and limited authentication and prevents replay attacks.



Bastion host is a specialized server designed to act as a gateway between an internal network and external networks (like the internet). It provides controlled, secure access to critical resources by acting as a hardened and isolated system that enforces strong authentication and logging.

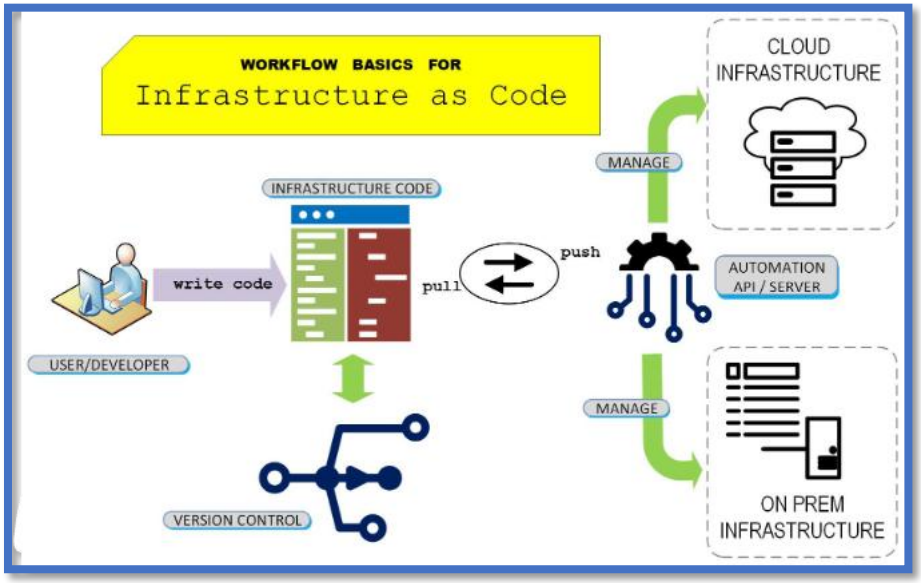


Virtual private cloud (VPC): is an on-demand configurable pool of shared resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations using the resources.

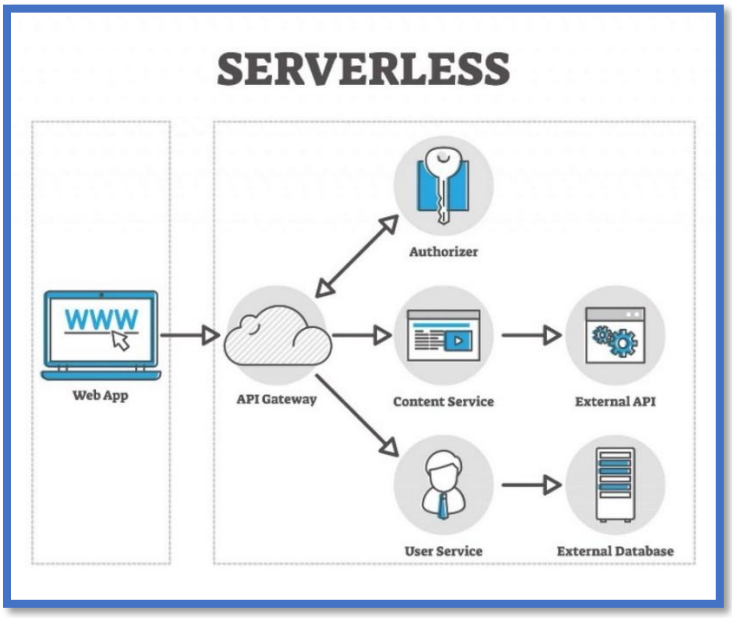


Security groups: In clouds, a security group is similar to an access control list (ACL) for network access. Security groups can be configured to control access to various elements of the cloud environment.

Infrastructure as Code (IaC) means managing your IT infrastructure (like servers, databases, and networks) using code, just like software. Instead of manually setting up hardware and configurations, you write scripts to automate these tasks. Ability to deploy infrastructure using scripts enables a feature of cloud computing known as *auto-scaling*.

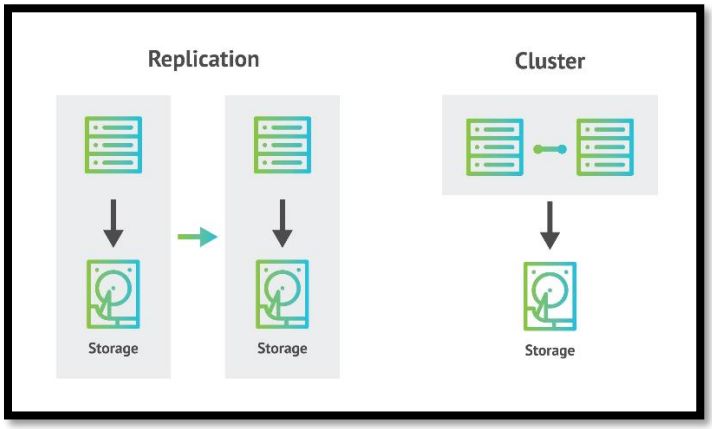


Serverless architecture is a cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software) or server is managed by the cloud service provider (CSP). There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. This is also known as ***a function as a service (FaaS)***.



Cluster is a group of hosts combined physically or logically by a centralized management system to allow for redundancy, configuration synchronization, failover, and the minimization of downtime. With a cluster, resources are pooled and shared between the members and managed as a single unit.

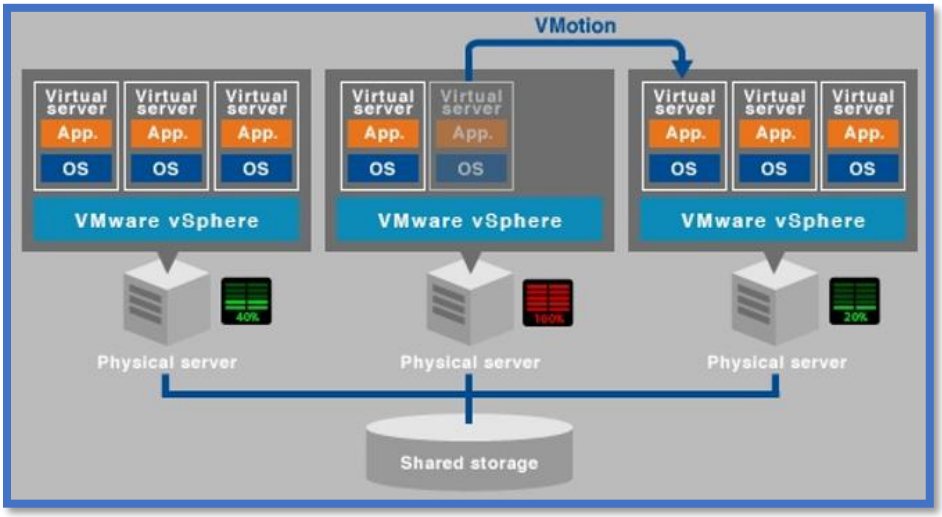
Clustering principles and technologies can be applied to a variety of computing resources, including applications, servers, networking appliances, and storage systems.



TIP

Data Center Temperature: 64° to 81° F (18° to 27° C)
Data Center Humidity: Dew point of 15° to 59° F (–9° to 15° C), relative humidity of 60%

Distributed Resource Scheduling (DRS): is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts. As loads change, virtual hosts can be moved between physical hosts to maintain the proper balance and done so in a way that is transparent to the users. Coordination element in a cluster of VMware ESXi hosts, which mediates access to physical resources and provides additional features supporting high availability and management.



Dynamic optimization is the process through which the cloud environment is constantly maintained to ensure that resources are available when and where needed and that physical nodes do not become overloaded or near capacity while others are underutilized.

Access controls should be implemented with a minimum of three layers:

- **Management plane:** These are your controls for managing access of users that directly access the cloud platform's management plane. For example, logging in to the web console of

an IaaS service will allow that user to access data in object storage. Fortunately, most cloud platforms and providers start with default deny access control policies.

- **Public and internal sharing controls:** If data is shared externally to the public or partners that don't have direct access to the cloud platform, there will be a second layer of controls for this access.
- **Application-level controls:** As you build your own applications on the cloud platform you will design and implement your own controls to manage access.

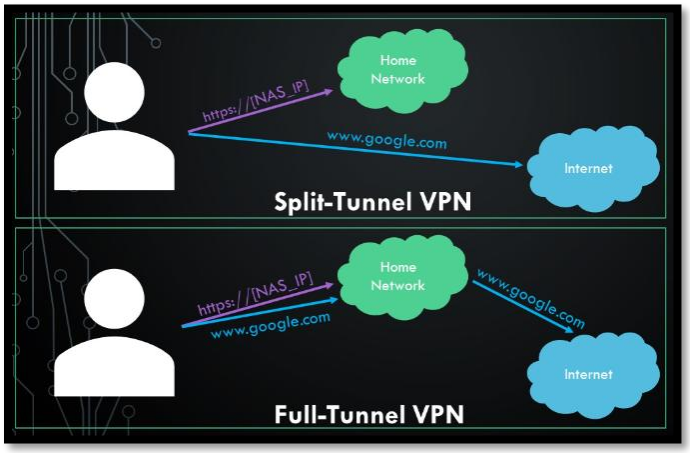
DISA STIGs: The US Defense Information Systems Agency (DISA) produces baseline documents known as Security Technical Implementation Guides (STIGs). These documents provide guidance for hardening systems used in high-security environments, and as such, may include configurations that are too restrictive for many organizations.

High Availability encompasses infrastructure and other supporting elements in addition to a system's uptime; high availability (HA) is defined by a robust system and infrastructure to ensure a system is not just up but also available. It is often measured as a number of 9s; for example, five nines or 99.999 percent availability.

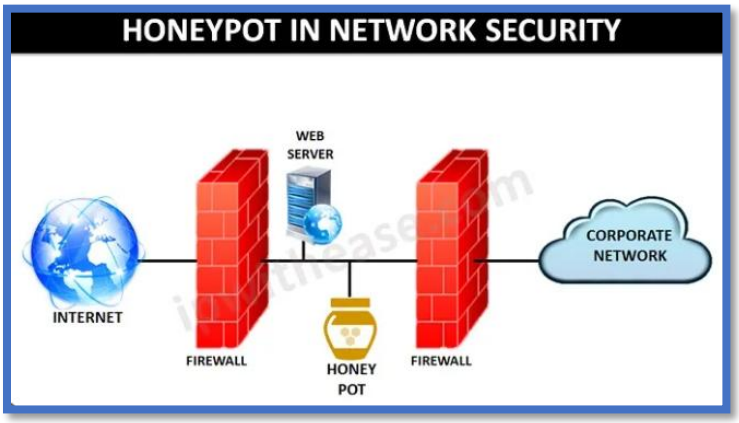
- **Tier 1** involves no redundancy and the most amount of downtime in the event of unplanned maintenance or an interruption. Expected to provide 99.671% availability.
- **Tier 2** provides partial redundancy, meaning an unplanned interruption will not necessarily cause an outage. Expected to provide 99.741% availability.
- **Tier 3** adds even more redundant components has a major advantage in that it never needs to be shut down for maintenance enough redundant components that any component can be taken offline for maintenance and data center continues to run expected to provide 99.982% availability.
- **Tier 4** N+1 and 2N+1 levels of redundancy can withstand either planned or unplanned activity without affecting availability. This is achieved by eliminating all single points of failure and requires fully redundant infrastructure, including dual commercial power feeds, dual backup generators expected to provide 99.995% availability.

Split tunnel vs full tunnel

- Split tunnel uses VPN for traffic destined for the corporate network only, and Internet traffic direct through its normal route.
- Full tunnel means using VPN for all traffic, both to the Internet and corporate network.



Honey Pot: A system that often has pseudo flaws and fake data to lure intruders. A group of honeypots is called a honeynet. Only ENTICE, not ENTRAP. You are not allowed to let them download items with "Enticement". For example, allowing download of a fake payroll file would be entrapment.



User Entity Behavior Analysis (UEBA): This is based on the interaction of a user that focuses on their identity and the data that they would normally access on a normal day. It tracks the devices that the user normally uses and the servers that they normally visit.

Sentiment Analysis: Artificial intelligence and machine learning to identify attacks. Cybersecurity sentiment analysis can monitor articles on social media, look at the text and analyze the sentiment behind the articles. Over time, can identify a users' attitudes to different aspects of cybersecurity.

Deep Learning: A subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks.

Predictive Analytics: A branch of advanced analytics used to make predictions about future events, via varying techniques from modeling, statistics, machine learning, data mining, and artificial intelligence.

Prescriptive Analytics: The use of technology to help organizations make informed decisions via the analysis of raw data. Prescriptive analytics tries to quantify the effect of future decisions in order to advise on possible outcomes before any decisions are actually made.

Non-Intrusive Scans: These are passive and merely report vulnerabilities. They do not cause damage to your system.

Intrusive Scans: Can cause damage as they try to exploit the vulnerability and should be used in a sandbox and not on your live production system.

Configuration Review: Configuration compliance scanners and desired state configuration in PowerShell ensure that no deviations are made to the security configuration of a system.

Vulnerability Scoring System

- ***Common Vulnerabilities and Exposures (CVE)*** provides a naming system for describing security vulnerabilities.
- ***National Vulnerability Database (NVD)*** is a database, maintained by NIST, that is synchronized with the MITRE CVE list.
- ***Common Vulnerability Scoring System (CVSS)*** provides a standardized scoring system for describing the severity of security vulnerabilities.
- ***Common Configuration Enumeration (CCE)*** provides a naming system for system configuration issues.
- ***Common Platform Enumeration (CPE)*** provides a naming system for operating systems, applications, and devices.
- ***Extensible Configuration Checklist Description Format (XCCDF)*** provides a language for specifying security checklists.
- ***Open Vulnerability and Assessment Language (OVAL)*** provides a language for describing security testing procedures.

Domain 6- Legal, Risk, and Compliance

Types Of Laws

- Criminal Law contains prohibitions against acts such as murder, assault, robbery, and arson.
- Civil Law (AKA Tort law) includes contract disputes, real estate transactions, employment, estate, and probate.
- Administrative Law Government agencies have some leeway to enact administrative law.
- Doctrine Law refers to a principle, framework, or body of rules established through judicial decisions or legal precedents.

General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and became enforceable in May 2018. It protects the personal data and privacy of EU citizens. The GDPR defines three relevant entities:

- **Data subject** the individual to whom the data pertains
- **Data controller** Any organization that collects data on EU residents
- **Data processor** Any organization that processes data for a data controller

The 7 data protection principles of GDPR are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitations
- Integrity and confidentiality
- Accountability

GDPR includes the following on data subject privacy rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (the so-called "right to be forgotten")
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

GDPR is directly binding on any corporation that processes the data of EU citizens, and will be adjudicated by the data supervisory authorities or the courts of the member states that have the closest relationship with the individuals or the entities on both sides of the dispute.

- **Applicability**: The GDPR applies to the processing of personal data in the context of the activities of the establishment of a controller or processor in the EU/EEA, regardless of whether the processing takes place in the EU/EEA or not. It also applies to the processing of personal data of data subjects who are in the EU/EEA by a controller or a processor not established in the EU/EEA if the processing relates to (a) the offering of goods or services irrespective of whether a payment by the data subject is required; or (b) the monitoring of the behavior of a data subject, when the behavior takes place within the EU/EEA.

- **Lawfulness:** The processing of personal data is allowed only if (a) the data subject has freely given specific, informed and unambiguous indication of his/her consent to the processing of his/her personal data, or (b) the processing is authorized by a statutory provision.
- **Accountability Obligations:** The GDPR has created numerous obligations for companies. For example, GDPR requires companies to keep records of their data processing activities. Certain categories of processing require a prior "Privacy Impact Assessment." Companies are expected to develop and operate their products and services in accordance with "privacy by design" and "privacy by default" principles.
- **Data Subjects' Rights**: Data subjects have rights to information regarding the processing of their data: the right to object to certain uses of their personal data; to have their data corrected or erased; to be compensated for damages suffered as a result of unlawful processing; the right to be forgotten; and the right to data portability. The existence of these rights significantly affects cloud service relationships.
- **Cross-border Data Transfer Restrictions**: The transfer of personal data outside the EU/EEA to a country that does not offer a similar range of protection of personal data and privacy rights is prohibited. To prove that it will be offering the "adequate level of protection" required, a company may use one of several methods, such as executing Standard Contractual Clauses (SCC), signing up to the EUUS Privacy Shield, obtaining certification of Binding Corporate Rules (BCRs), or complying with an approved industry Code of Conduct or approved certification mechanism. In rare cases, the transfer might be affected with the explicit, informed, consent of the data subject, or if other exceptions apply.
- **Breaches of Security**: The GDPR requires companies to report that they have suffered a breach of security. The reporting requirements are risk-based, and there are different requirements for reporting the breach to the Supervisory Authority and to the affected data subjects. Breaches must be reported within 72 hours of the company becoming aware of the incident.
- **Discrepancies among Member States**: There are numerous instances where each member state may adopt its own rules. For example, Germany requires that a Data Protection Officer be appointed if the company has more than nine employees.
- **Sanctions:** Violations of the GDPR expose a company to significant sanctions. These sanctions may reach up to the greater of four percent of their global turnover or gross income, or up to EUR 20 million.

Network Information Security Directive (NIS Directive) The NIS Directive entered into force in August 2016, requiring each EU/EEA member state to implement the Directive into its national legislation by May 2018. The NIS Directive establishes a framework to enable networks and information systems to resist, at a given level of confidence, actions that compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or the related services that are offered by or accessible through those networks and information systems.

- Taking technical and organizational measures to manage risks posed to the security of networks and information systems used in their operations.
- Taking appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems used for the provision of such essential services, to facilitate the continuation of those services.
- Notifying, without undue delay, the competent authorities or agencies of incidents having a significant impact on the continuity of the essential services they provide.

- Providing information is necessary to assess the security of their networks and information systems.
- Providing evidence of the effective implementation of security policies, such as the results of a security audit.

Organization for Economic Cooperation and Development (OECD) Privacy Guidelines *are a set of principles developed to protect privacy and personal data while enabling international data flows.*

- **Collection limitation principle**: There should be limits on the collection of personal data as well as consent from the data subject.
- **Data quality principle:** Personal data should be accurate, complete, and kept up to date.
- **Purpose specification principle:** The purpose of data collection should be specified, and data use should be limited to these stated purposes.
- **Use limitation principle:** Data should not be used or disclosed without the consent of the data subject or by the authority of law.
- **Security safeguards principle:** Personal data must be protected by reasonable security safeguards against unauthorized access, destruction, use, or disclosure.
- **Openness principle:** Policies and practices about personal data should be freely disclosed, including the identity of data controllers.
- **Individual participation principle:** Individuals have the right to know if data is collected on them, access any personal data that might be collected, and obtain or destroy personal data if desired.
- **Accountability principle:** A data controller should be accountable for compliance with all measures and principles.

Asia Pacific Economic Cooperation Privacy Framework (APEC) is a regional framework designed to promote the protection of personal information while enabling cross-border data flows among APEC member economies. It provides guidance for harmonizing privacy laws and fostering trust in the digital economy across the Asia-Pacific region. Includes 21 economies such as the United States, China, Japan, Australia, Singapore, and Canada.

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

Payment Card Industry Data Security Standard (PCI DSS): The current standard version 3.2 affects companies that accept, process, or receive electronic payments. The following are the requirements of PCI-DSS.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public network

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and application

Implement Strong Access Control Measure

7. Restrict access to cardholder data by business on a need-to-know basis
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Privacy Shield: This provides a voluntary privacy compliance framework through which companies can comply with portions of the GDPR in order to facilitate the movement of EU citizens' data into the United States by companies based in the United States. Note that this agreement is facing legal challenges in the EU. Privacy Shield seven principles are as follows:

- Notice
- Choice
- Accountability for onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, enforcement, and liability

Sarbanes–Oxley Act (SOX): U.S. public companies to protect financial data when stored and used. It is intended to protect shareholders of the company as well as the general public from accounting errors or fraud within enterprises. This act specifically applies to publicly traded companies and is enforced by the Securities and Exchange Commission (SEC). It is applicable to cloud practitioners in particular because it specifies what records must be stored and for how long, internal control reports, and formal data security policies. Focuses on financial transparency and accountability for public companies. ***SOX*** emphasizes **financial accountability** and integrity within public companies.

- **Section 802:** It is a crime to destroy, change, or hide documents to prevent their use in official legal processes.
- **Section 804**: Companies must keep audit-related records for a minimum of five years.

Gramm–Leach–Bliley Act (GLBA): U.S. federal law focuses on protecting consumers' financial information in the financial sector (Banks, credit unions, mortgage brokers, investment firms, insurance companies, payday lenders, and financial advisors). Up to $100,000 per violation for institutions & $10,000 per violation for individuals. Individuals can face up to 5 years of imprisonment for severe violations. ***GLBA*** focuses on protecting **consumer financial data** and ensuring privacy for individuals.

- The Financial Privacy Rule, which regulates the collection and disclosure of private financial information.
- The Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information.

- The Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses)

Family Education Rights and Privacy Act (FERPA): deals with privacy rights for students, and the Federal Information Security Management Act (FISMA), which protects federal data privacy.

State data privacy laws, which now exist in all 50 states as well as U.S. territories.

Clarifying Lawful Overseas Use of Data (CLOUD) Act is a U.S. law enacted in 2018. It establishes rules about how law enforcement agencies can access data stored by tech companies, even if that data is located outside the United States. The act aims to clarify cross-border data access issues while balancing privacy concerns and international cooperation.

New York State Department of Financial Services (NY DFS) cybersecurity framework for the financial industry (23 NYCRR 500).

NIST 800-171: mostly dealing with contractor compliance to do business with the government.

Contractual private data refers to sensitive and confidential information that is exchanged or documented within the scope of a legal contract. Such as legal contracts, intellectual property (IP), financial statements, trade secrets etc.

Regulated private data refers to sensitive personal or business information governed by specific laws, regulations, or standards to ensure its protection, confidentiality, and ethical handling. Such as PII, PHI, Financial data, PCI data etc...

Contractual requirements

- Payment Card Industry Data Security Standard (PCI DSS)
- Financial Industry Regulatory Authority (FINRA)
- Service Organization Controls (SOC)
- Generally Accepted Privacy Principles (GAPP)
- Center for Internet Security (CIS) Critical Security Controls (CSC)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

eDiscovery is defined as any process in which electronic data is pursued, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. In a typical eDiscovery case, computing data might be reviewed offline (with the equipment powered off or viewed with a static image) or online (with the equipment on and accessible).

eDiscovery Investigations

- SaaS-based eDiscovery
- Hosted eDiscovery: limit a customer to a preselected list of forensic solutions, as CSPs are often wary of customer-provided tools due to the potential for affecting other cloud customers during the process.
- Third-party eDiscovery

Cloud Forensics and Standards

- **Cloud Security Alliance:** The CSA Security Guidance Domain 3: Legal Issues: Contracts and Electronic Discovery highlights some of the legal aspects raised by cloud computing.

- **ISO/IEC 27037:2012**: This provides guidelines for the handling of digital evidence, which include the identification, collection, acquisition, and preservation of data related to a specific case.
- **ISO/IEC 27041:2014-01**: This provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose."
- **ISO-IEC 27042:2014-01:** This standard is a guideline for the analysis and interpretation of digital evidence.
- **ISO/IEC 27043:** The security techniques document covers incident investigation principles and processes.
- **ISO/IEC 27050-1:** This standard covers electronic discovery, the process of discovering pertinent electronically stored information involved in an investigation.

Evidence Attributes

- **Authentic**: The information should be genuine and clearly correlated to the incident or crime.
- **Accurate:** The truthfulness and integrity of the evidence should not be questionable.
- **Complete:** All evidence should be presented in its entirety, even if it might negatively impact the case being made.
- **Convincing:** The evidence should be understandable and clearly support an assertion being made.
- **Admissible:** Evidence must meet the rules of the body judging it, such as a court. Hearsay (indirect knowledge of an action) or evidence that has been tampered with may be thrown out by a court.

Personal identifiable information (PII): is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (such as SSN numbers) that can identify a person uniquely, or quasi-identifiers (such as race) that can be combined with other quasi-identifiers (such as date of birth) to successfully recognize an individual.

Protected health information (PHI) also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Heath Insurance Portability and Accountability Act (HIPAA): This 1996 U.S. law regulates the privacy and control of health information data.

Australian Privacy Act: organizations may process data belonging to Australian citizens offshore. transferring entity (the data owner) must ensure that the receiver of the data holds and processes it in accordance with the principles of Australian privacy law.

Personal Information Protection and Electronic Documents Act (PIPEDA) a national level law that restricts how commercial businesses may collect, use, and disclose personal information. PIPEDA covers information about an individual that is identifiable to that specific individual. DNA, age, medical, education, employment, identifying numbers, religion, race/ethnic origin, financial information.

California Consumer Protection Act (CCPA), the strongest state privacy law in the nation.

- Know what personal data is being collected about them
- Know whether their personal data is sold or disclosed and to whom

- Opt out of the sale of personal data
- Access their personal data
- Request a business to delete any personal information about a consumer collected (the right to be forgotten)
- Be protected from discrimination (by service or price) for exercising their privacy rights

Stored Communication Act (SCA), as enacted as Title II of the Electronic Communication Privacy Act, created privacy protection for electronic communications (such as email or other digital communications) stored on the Internet. In many ways, this act extends the Fourth Amendment of the U.S. Constitution.

ISO/IEC 27017 -A security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.

ISO/IEC 27018 – addresses the **privacy** aspects of cloud computing

- **Consent:** Personal data obtained by a CSP may not be used for marketing purposes unless expressly permitted by the subject. A customer should be permitted to use a service without requiring this consent.
- **Control:** Customers shall have explicit control of their own data and how that data is used by CSP.
- **Transparency**: CSPs must inform customers of where their data resides AND any subcontractors that may process personal data.
- **Communication:** Auditing should be in place, and any incidents should be communicated to customers.
- **Audit**: Companies (CSP, in this case) must subject themselves to an independent audit on an annual basis.

ISO/IEC 27701 -Extends the ISMS guidance in 27001 to manage risks related to privacy, by implementing and managing a privacy information management system (PIMS).

ISO/IEC 27036 is a multi-part international standard that provides comprehensive guidelines for managing information security within supplier relationships.

Generally Accepted Privacy Principles (GAPP) consists of 10 principles for privacy from the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). Widely incorporated into the SOC 2 framework as an optional criterion. GAPP provides guidelines for designing, implementing, and managing privacy practices to protect personal information.

1. **Management**
2. **Notice**
3. **Choice and consent**
4. **Collection**
5. **Use, retention, and disposal**
6. **Access**
7. **Disclosure to third parties**
8. **Security for privacy**
9. **Quality**
10. **Monitoring and enforcement**

Privacy impact assessment (PIA) is designed to identify the privacy data being collected, processed, or stored by a system, and assess the effects of data breach. To conduct a PIA, you must define assessment scope, data collection methods, and plan for data retention.

Privacy Level Agreement
In this context, the CSA has defined baselines for compliance with data protection legislation and leading practices with the realization of a standard format named by the Privacy Level Agreement (PLA). By means of the PLA, the service provider declares the level of personal data protection and security that it sustains for the relevant data processing. The PLA, as defined by the CSA, does the following:

- Provides a clear and effective way to communicate the level of personal data protection offered by a service provider.
- Works as a tool to assess the level of a service provider's compliance with data protection legislative requirements and leading practices.
- Provides a way to offer contractual protection against possible financial damage due to lack of compliance.

FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government program designed to standardize the approach to security assessment, authorization, and continuous monitoring for cloud services used by federal agencies. It ensures that cloud services meet stringent security requirements before being used to handle federal data.

SSAE (Statement on Standards for Attestation Engagements) is a set of standards defined by the AICPA to be used when creating SOC reports. The most current version is SSAE 18.

ISAE (International Auditing and Assurance Standards Board 3402) reports are very similar in nature and structure to the SOC type 2 reports, and they are also designed to be a replacement for the SAS 70 reports. Like SOC reports, the ISAE reports have two subtypes:

- **Type 1 reports** these are aligned with SOC type 2 reports in that they are based on a snapshot of a single point in time.
- **Type 2 reports** These are also aligned with SOC type 2 reports in scope and intent, and they are done typically for six months to show the management and use of controls over that period.

Cloud Security Alliance (CSA) offers a **Security Trust Assurance and Risk (STAR)** certification that can be used by cloud service providers, cloud customers, or auditors and consultants to ensure compliance with the desired level of assurance. STAR consists of three levels of certification:

- **Level 1**: Self-Assessment is a complimentary offering that documents the security controls provided by various cloud computing offerings, helping users assess the security of cloud providers they currently use or are considering using.
- **Level 2**: Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. STAR Attestation provides rigorous third-party independent assessments of cloud providers.
- **Level 3:** Continuous monitoring through automated processes that ensure security controls are monitored and always validated.

CSA Notorious Nine		
Threat	**Impact**	**Mitigation**
Data Breaches	Loss of sensitive data	Encryption, strong access controls
Data Loss	Irrecoverable data	Backups, retention policies
Account Hijacking	Unauthorized access	MFA, account activity monitoring
Insecure Interfaces/APIs	System exploitation	API authentication, secure development practices
Denial of Service (DoS)	Service disruption	DDoS protection, traffic monitoring
Malicious Insiders	Internal data misuse	Least privilege, user activity monitoring
Abuse of Cloud Services	Cybercriminal activity	Cloud activity monitoring, automated abuse detection
Insufficient Due Diligence	Poor provider security	Risk assessments, vendor evaluations
Shared Tech Vulnerabilities	Cross-tenant data breaches	Provider isolation mechanisms, frequent patching

Consensus Assessments Initiative Questionnaire (CAIQ) is a standardized security assessment tool developed by the Cloud Security Alliance (CSA). It is designed to help organizations evaluate the security and compliance of cloud service providers (CSPs) by providing a structured way to gather information about their security practices and controls.

Audit Scope

- Statement of purpose and objectives
- Scope of audit and explicit exclusions
- Type of audit
- Security assessment requirements
- Assessment criteria and rating scales
- Criteria for acceptance
- Expected deliverables
- Classification (for example, secret, top secret, public, etc.)

Audit Process

The four phases of an audit consist of the following:

- Audit planning
  - Documentation and definition of audit objectives. This process is a collaborative effort to define what standards are being measured.
  - Addressing concerns and risks.
  - Defining audit output formats.
  - Identifying auditors and qualifications.
  - Identifying scope and restrictions.
- Audit fieldwork
  - Conducting general controls, walk-throughs and risk assessments.
  - Interviewing key staff on procedures.

- Conducting audit test work, which may include physical and architectural assessments with software tools.
- Ensuring criteria are consistent with SLA and contracts.

- Audit reporting
  - Conduct meetings with management to discuss findings.
  - Discussing recommendations for improvement.
  - Allowing for departmental response to findings.
- Audit follow-up
  - Additional inquiry or testing could be performed to ensure compliance to recommendations.
  - Identify lessons learned in the audit process.

Information security management system (ISMS) is a systematic approach to information security consisting of processes, technology, and people designed to help protect and manage an organization's information. These systems are designed to strengthen the three aspects of the CIA triad: confidentiality, availability, and integrity. An ISMS is a powerful risk management tool in place at most medium and large organizations.
ISO 27001:2013 information security standards controls.

- A.5 Information security policies: How policies are written and reviewed
- A.6 Organization of information security: The assignment of responsibilities for specific tasks
- A.7 Human resource security: Ensuring that employees understand their responsibilities prior to employment and once they've left or changed roles
- A.8 Asset management: Identifying information assets and defining appropriate protection responsibilities
- A.9 Access control: Ensuring that employees can only view information that's relevant to their job role
- A.10 Cryptography: The encryption and key management of sensitive information
- A.11 Physical and environmental security: Securing the organization's premises and equipment
- A.12 Operations security: Ensuring that information processing facilities are secure
- A.13 Communications security: How to protect information in networks
- A.14 System acquisition, development and maintenance: Ensuring that information security is a central part of the organization's systems
- A.15 Supplier relationships: The agreements to include in contracts with third parties and how to measure whether those agreements are being kept
- A.16 Information security incident management: How to report disruptions and breaches and who is responsible for certain activities
- A.17 Information security aspects of business continuity management: How to address business disruptions
- A.18 Compliance: How to identify the laws and regulations that apply to your organization

National Institute of Standards (NIST) cybersecurity framework CSF (v1.1). This framework identifies controls in these five broad areas:

- Identify
- Protect
- Detect
- Respond
- Recover

Organizational Policies

- Financial losses
- Loss of data
- Reputational damage
- Statutory and regulatory compliance issues
- Abuse or misuse of computing systems and resources

Functional Policies

- Data classification policies: Identifies types of data and how each should be handled
- Network services policies: How issues such as remote access and network security are handled
- Vulnerability scanning policies: Routines and limitations on internal scanning and penetration testing
- Patch management policies: How equipment is patched on what schedule
- Acceptable use policies: What is and is not acceptable to do on company hardware and networks
- Email use policies: What is and is not acceptable to do on company email accounts
- Password policies: Password complexity, expiration, reuse
- Incident response policies: How incidents are handled

Cloud Computing Policies

- Password policies: If an organization has password policies around length, complexity, expiration, or multifactor authentication (MFA), it is important to ensure that these same requirements are met by a cloud service provider.
- Remote access: The same bar must be met for remote access to cloud providers as on-premises services. This may include items such as up-to-date patching, hard disk encryption, or MFA.
- Encryption: Policies about encryption strength and when encryption is required. Key escrow can be an important aspect of policy to focus on (for example who has the decryption keys?).
- Data backup and failover: Policies on data retention and backup must be enforced on cloud providers. If policies exist on data location for backups and redundancy, they must also be enforced on CSPs.
- Third-party access: What third parties might have access to data stored with the CSP? Can this access be logged and audited?
- Separation of duties: Can controls for the separation of key roles be enforced and maintained by the cloud provider?
- Incident response: What are the required steps in a response, including who is contacted for a variety of incidents?

Risk Management

- **Risk appetite** is the total amount of risk that an organization is willing to shoulder in aggregating across all assets.
- **Risk capacity** is the level of risk an organization can shoulder.
- **Risk tolerance** is the amount or level of risk that an organization will accept per individual asset-threat pair.

- **Risk Avoidance** is the process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option. For example, is to locate a business in Arizona instead of Florida to avoid hurricanes.
- **Risk Acceptance**: Accepting risk, or acceptance of risk, is the result after a cost/benefit analysis shows countermeasure costs would outweigh the possible cost of loss due to a risk. It also means that management has agreed to accept the consequences and the loss if the risk is realized.
- **Risk Rejection** An unacceptable possible response to risk is to reject risk or ignore risk. Denying that a risk exists and hoping that it will never be realized are not valid or prudent due care/due diligence responses to risk. Rejecting or ignoring risk may be considered negligence in court.
- **Inherent risk** is the level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed.

Metrics for Risk Management

- **Patching levels**: How many devices on your cloud networks are fully patched and up-to-date?
- **Intrusion attempts**: How many times have unknown actors tried to breach your cloud systems?
- **Mean time to detect (MTTD)**: How long does it take for security teams to become aware of a potential security incident?
- **Mean time to contain (MTTC)**: How long does it take to contain identified attack vectors?
- **Mean time to resolve (MTTR)**: How long until security threats are definitively dealt with?
- **Days to patch**: How long does it take a security team to fully patch a cloud system?
- **Access management**: How many users have administrative access?

RISK= Threat Likelihood* Magnitude of Impact

NIST special publication 800-37 Revision 2 is a framework for managing information system risks through a structured Risk Management Framework (RMF). The publication focuses on integrating risk management into the system development life cycle (SDLC) and ensuring security and privacy controls are effectively implemented.

Step	Description
1. Prepare	Establish the organization's readiness by assigning roles, defining resources, and conducting risk assessments. Align risk management with organizational goals and set the context for RMF implementation.
2. Categorize	Determine the sensitivity and criticality of the information system and data. Use FIPS 199 standards to define the system's impact level (low, moderate, or high).
3. Select	Choose security and privacy controls from NIST SP 800-53 based on the system's risk categorization. Tailor controls to meet specific needs.
4. Implement	Integrate and deploy selected controls into the system. Document how controls are implemented to meet security and privacy requirements.
5. Assess	Evaluate the effectiveness of the implemented controls to ensure they meet the necessary requirements. Identify any gaps or deficiencies.

6. Authorize	Senior leaders (Authorizing Officials) review the system's risk posture and decide whether to approve it for operation based on the identified residual risks.
7. Monitor	Continuously track and assess the system's security and privacy posture. Update controls and respond to changes in risks, threats, or system conditions.

ISO 31000, "Risk management - Guidelines," was first published in 2009 and majorly revised in 2018.

- Avoiding risk by deciding not to start or continue with the activity that gives rise to risk
- Accepting or increasing the risk to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

European Network and Information Security Agency (ENISA) produces a number of useful resources, and the "Cloud Computing Risk Assessment (2009)". ENISA spells out 53 types of vulnerabilities that companies should be aware of, and a top eight security risk list based on the impact and likeliness of occurrence. The top eight security risks include the following:

1. **Loss of governance**: Gaps in the security defenses caused by differences in the understanding of responsibility between the client and the CSP.
2. **Vendor Lock-in**: The difficulty in leaving CSP.
3. **Vendor lock-out** refers to a situation where an organization becomes overly reliant on a single cloud provider, making it difficult, expensive, or disruptive to migrate services, applications, or data to another provider or bring them back on-premises.
4. **Isolation failure**: The potential failures caused by lack of separation in storage, memory, and other hardware between cloud clients.
5. **Compliance risk**: The CSP provides a new challenge to achieving certification.
6. **Management interface compromise**: Management interfaces for cloud environments provide an additional attack vector.
7. **Data protection**: How CSPs handle data in a lawful way.
8. **Insecure data deletion**: Secure deletion of the cloud is complicated by its distributed nature.
9. **Malicious insiders**: Addition of a CSP adds high-risk access individuals who can comprise cloud architectures and data.

Cloud Certification Schemes List (CCSL): The CCSL is a comprehensive list of existing certification schemes relevant to cloud computing customers.

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 2
- FedRAMP
- PCI DSS
- CSA STAR

- C5 (Germany)
- GDPR

Cloud Certification Schemes List and Meta framework (CCSM) is a meta-framework that maps detailed security requirements used in the public sector to the security objectives of existing cloud certification schemes.

NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing.
NIST SP 800-145: Defines cloud computing service and deployment models.
NIST SP 800-146: Cloud Computing Synopsis and Recommendations.
NIST SP 500-291: Cloud Computing Standards Roadmap.
NIST SP 500-292: Cloud Computing Reference Architecture.
NIST SP 500-293: Cloud Computing Technology Roadmap.

ISO 15408-1:2009: The Common Criteria

- **Target of evaluation (ToE)** – The system or product that is being evaluated.
- **Security target (ST)** – The documentation describing the ToE, including the security requirements and operational environment.
- **Protection profile (PP)** – An independent set of security requirements and objectives for a specific category of products or systems, such as firewalls or intrusion detection systems.
- **Evaluation assurance level (EAL)** – The evaluation score of the tested product or system.

Vendor Management

- Initial contract negotiations
- Service level agreement monitoring and project coordination
- User community communications
- Security and business processes
- Upgrades

Contract Management

- Access to systems
- Backup and disaster recovery
- Data retention and disposal
- Definitions
- Incident response
- Litigation
- Metrics
- Performance requirements
- Regulatory and legal requirements
- Security requirements
- Termination

Contracting Documents

- **Master service agreements (MSAs)** provide an umbrella contract for the work that a vendor does with an organization over an extended period.

- **Service-level agreements (SLAs)** are written contracts that specify the conditions of service that will be provided by the vendor and the remedies available to the customer if the vendor fails to adhere to the SLA.
- **Memorandum of understanding (MOU)** is a letter written to document aspects of the relationship.
- **Statement of Work (SOW)** is a formal document that defines the scope, objectives, deliverables, timeline, and responsibilities for a specific project or service agreement. It is often used in business relationships between clients and service providers, contractors, or vendors to ensure mutual understanding and accountability.
- **Business partnership agreements (BPAs)** exist when two organizations agree to do business with each other in a partnership.
- **Nondisclosure agreements (NDAs)** protect the confidentiality of information used in the relationship.

Cyber Risk Insurance is designed to help an organization modify risk by sharing the risk of a cyber incident with others via a policy that might offset costs involved with recovery after a cyber-related security incident such as a breach.

- **Investigation**: Costs associated with the forensic investigation to determine the extent of an incident. This often includes costs for third-party investigators.
- **Direct business losses**: Direct monetary losses associated with downtime or data recovery, overtime for employees, and oftentimes, reputational damage to the company.
- **Legal notifications**: Costs associated with required privacy and breech notifications required by relevant laws.
- **Lawsuits**: Policies can be written to cover losses and payouts due to class action or other lawsuits against a company after a cyber incident.
- **Extortion**: The insurance to pay out ransomware demands is growing in popularity. This may include direct payments to ensure data privacy or accessibility by the company.

Supply chain should always be considered in any business continuity or disaster recovery planning. The same concepts of understanding dependencies, identifying single points of failure, and prioritizing services for restoration are important to apply to the entire supply chain. This includes the cloud services a company may employ to deliver their services and the associated third parties that enable that cloud provider.

ISO 27036: Information Security for Supplier Relationships.

NIST IR 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.

NIST SP 800-61 rev2: Computer Security Incident Handling Guide.

NIST SP800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

ENISA-2015 publication on supply chain integrity.

NERC/CIP: North American Electric Reliability Corporation Critical Infrastructure Protection regulates organizations involved in power generation and distribution.

Consumer Data Protection Act (CDPA) is a legal framework designed to protect the personal data and privacy of individuals.

Virginia Consumer Data Protection Act (VCDPA) is a widely recognized law in the United States focusing on consumer rights and business responsibilities regarding personal data.

Export Administration Regulations (EAR) are a set of regulations enforced by the U.S. Department of Commerce. The EAR governs the export, re-export, and transfer (in-country) of commercial items, including some "dual-use" goods, technology, and software that have both civilian and military applications.

International Traffic in Arms Regulations (ITAR) governs the export, re-export, and transfer of defense-related articles, services, and technical data to ensure that sensitive military and defense-related technologies.

Wassenaar Arrangement promotes "international security and stability" by regulating exchanges of conventional weapons such as guns, bombs, torpedoes, grenades, and mines; dual-use goods; and technologies. The agreement was revised to address cyber weapons, including malicious software, command-and-control software, and Internet surveillance software.

Organizational Normative Framework (ONF) is a comprehensive structure of policies, standards, procedures, and guidelines that govern the operations of an organization to achieve its objectives while maintaining compliance with regulations, mitigating risks, and adhering to best practices.

Application Normative Framework (ANF) is a structured set of policies, standards, procedures, and best practices designed to govern the secure development, deployment, and maintenance of software applications. It ensures that applications meet organizational requirements, comply with regulatory standards, and address security, performance, and quality objectives.

American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) is a global professional association dedicated to advancing the arts and sciences of heating, ventilation, air conditioning, and refrigeration (HVAC&R). ASHRAE focuses on sustainability, innovation, and energy efficiency in building systems and provides resources to improve indoor air quality, environmental sustainability, and operational efficiency.