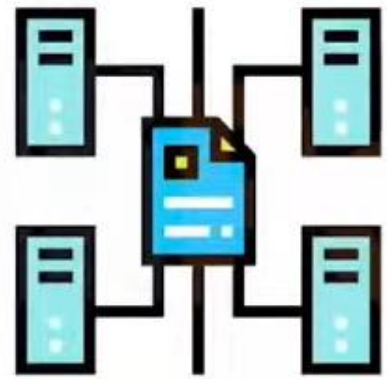
Cloud Data Policies

There needs to be policies that deal with several activities performed on data in cloud such as:

Retention Policies

Deletion Policies



Archiving Policies

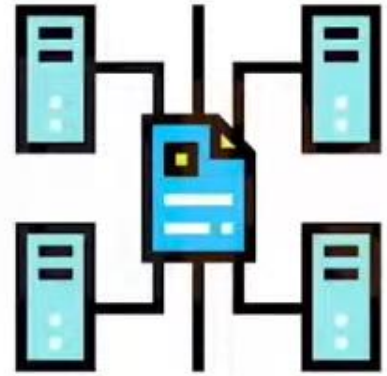
Legal Hold Policies

Cloud Data Policies

These specify how to securely delete data so that when a specific resource is assigned to a different user they should not be able to recover the deleted data

Retention Policies

Deletion Policies



Archiving Policies

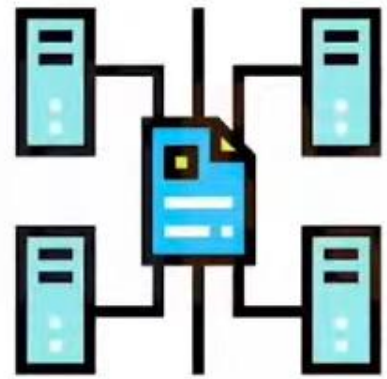
Legal Hold Policies

Cloud Data Policies

These specify how long the data needs to be dormant before it is archived, how long does the archived data needs to be stored etc.

Retention Policies

Deletion Policies



Archiving Policies

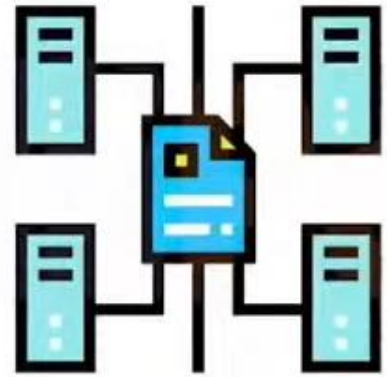
Legal Hold Policies

Cloud Data Policies

Some data is higly sensitive in a legal context which should be stored in within specified regions, with specified encrption policies etc. These regulations must be followed

Retention Policies

Deletion Policies

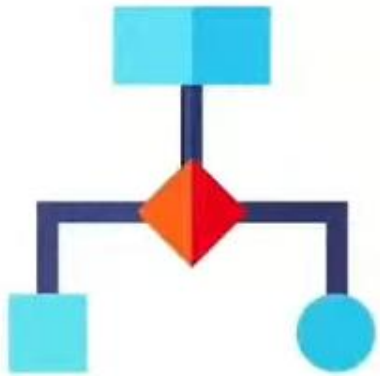


Archiving Policies

Legal Hold Policies

Cloud Data Events

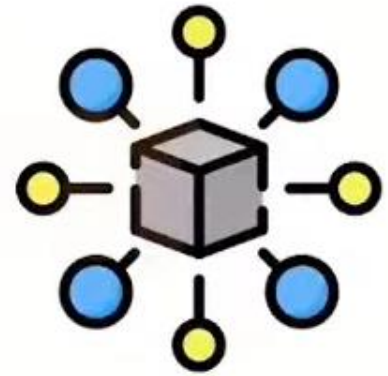
Data Events are events or notifications caused by creation, modification or deletion of data. There are several factors associated with data events, such as:



Event Sources

Analysis

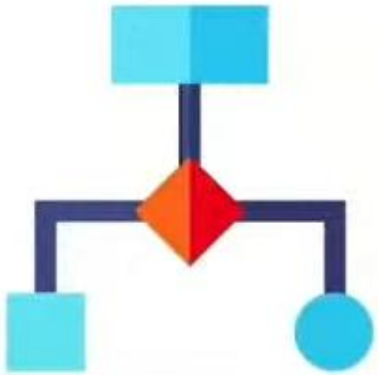
Non Repudiation



Chain of Custody

Cloud Data Events

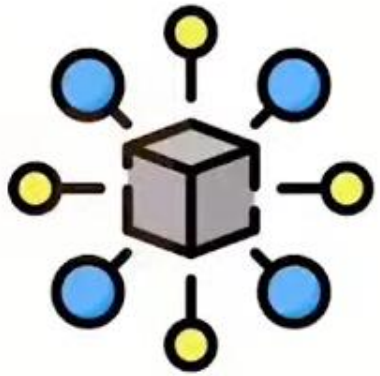
Event Sourcing is the process of keeping track of all the information regarding changes made to some data in a system and event sources are soft wares that save or log this information



Event Sources

Analysis

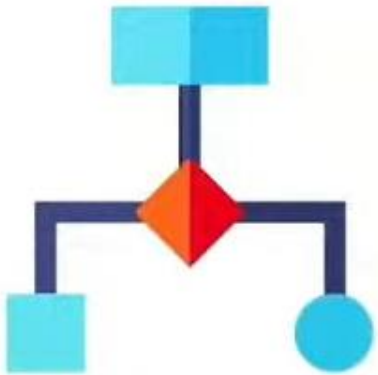
Non Repudiation



Chain of Custody

Cloud Data Events

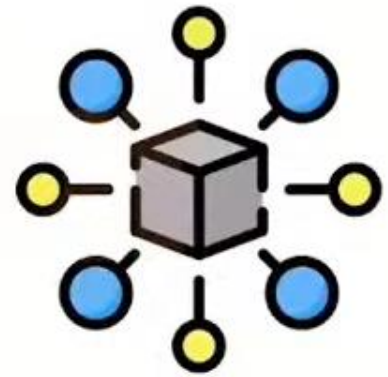
These data events need to be properly logged stored and analyzed, you can also create dash boards for visualization of this data



Event Sources

Analysis

Non Repudiation



Chain of Custody

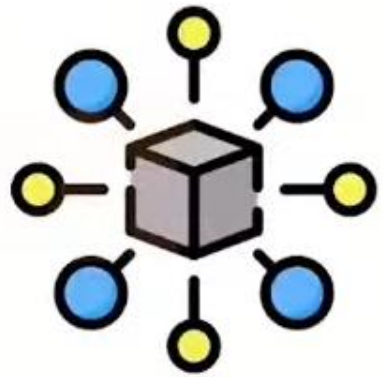
Cloud Data Events

Non Repudiation is a situation where a customer cannot deny authorship of some data and its event

Event Sources

Analysis

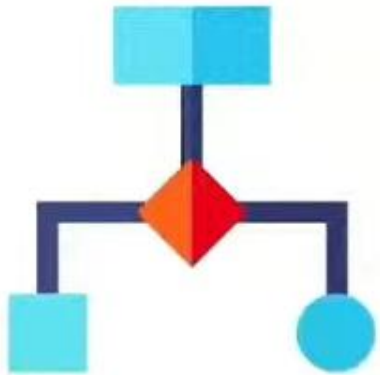
Non Repudiation



Chain of Custody

Cloud Data Events

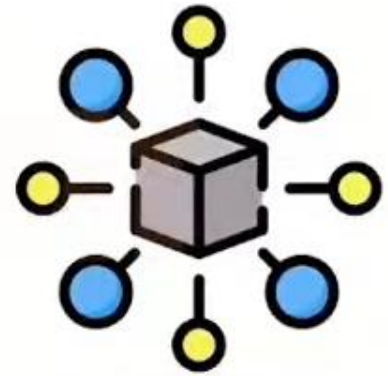
Chain of custody refers to the documentation that establishes a record of the control, transfer, and disposition of control of data



Event Sources

Analysis

Non Repudiation



Chain of Custody

Cloud Concepts

It involved numerous complicated tasks such as:

Understanding hardware Requirements

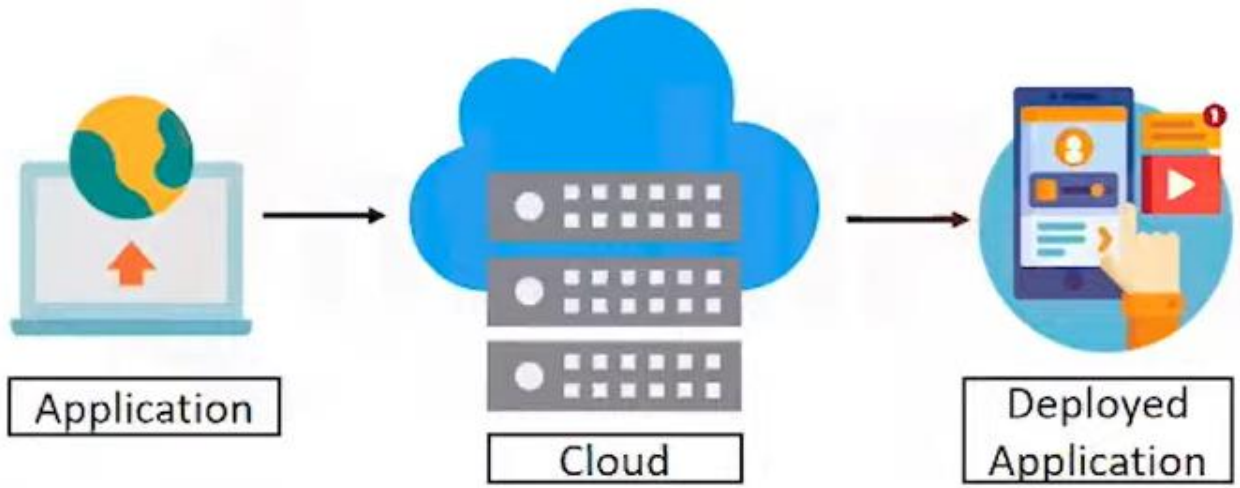
Buying required hardware

Setting up the infrastructure

Configuring the systems

Cloud Concepts

Cloud computing simply removes all the roadblocks you come across when you need access to some extra computing resources



To put it simply, cloud computing refers to the delivery of computing services over a network to a remote customer

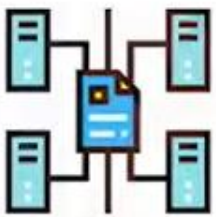
Cloud Concepts

Cloud computing also offers several advantages such as

On Demand

Scalable

Elasticity



Broad Network Access

Measured Services

Multi-Tenancy

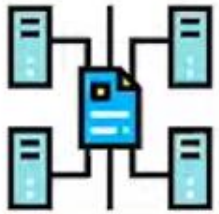
Resource Pooling

Cloud Concepts

On Demand

Scalable

Elasticity



Broad Network Access

Measured Services

Multi-Tenancy

Resource Pooling

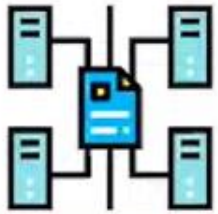
- Anyone can access cloud computing services anytime they need to
- Before cloud computing, anyone in need of computation resources had to buy these resources and configure them which took time

Cloud Concepts

On Demand

Scalable

Elasticity



Broad Network Access

Measured Services

Multi-Tenancy

Resource Pooling

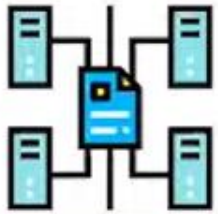
- Cloud computing allows you to increase the capacity of resources and services quite easily
- This can be done by either horizontal scaling or vertical scaling
  In horizontal scaling we add more servers to our pool (cluster) of servers
- In vertical scaling we add more resources to our existing servers

Cloud Concepts

On Demand

Scalable

Elasticity



Broad Network Access

Measured Services

Multi-Tenancy

Resource Pooling

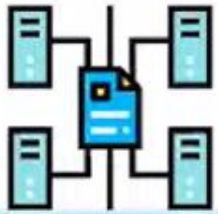
- With cloud computing we can grow or shrink compute capacity as we need them
- This is especially useful during times of high traffic when we need more computing power only for a short period of time

Cloud Concepts

On Demand

Scalable

Elasticity



Broad Network Access

Measured Services

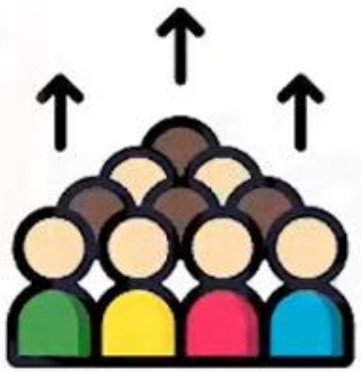
Multi-Tenancy

Resource Pooling

- Cloud Computing Services are available to be accessed anywhere using the internet
- You do not need to be on a special on premise network to access these services

Cloud Computing Roles

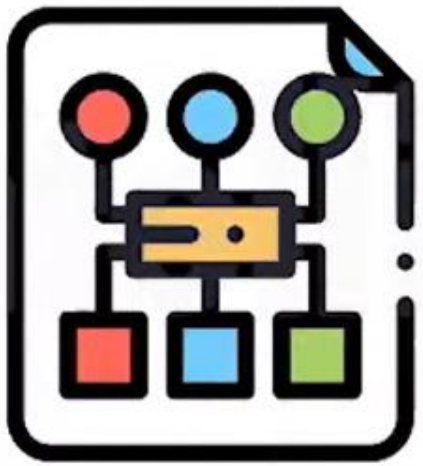
There are four main cloud computing roles which we need to be aware of



Provider	Customer	Partner	Broker

Cloud Building Blocks

To understand cloud security, what is most important is that we understand basic building blocks of cloud computing



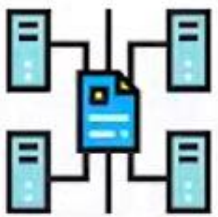
These building blocks are nothing but the infrastructure services that make up the various cloud computing platforms

Cloud Building Blocks

These building blocks are:

Compute

Storage

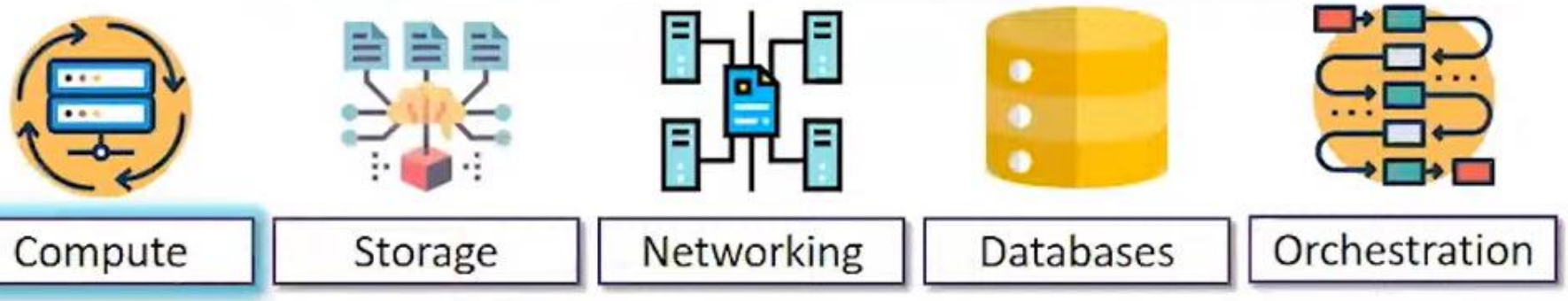


Networking

Databases

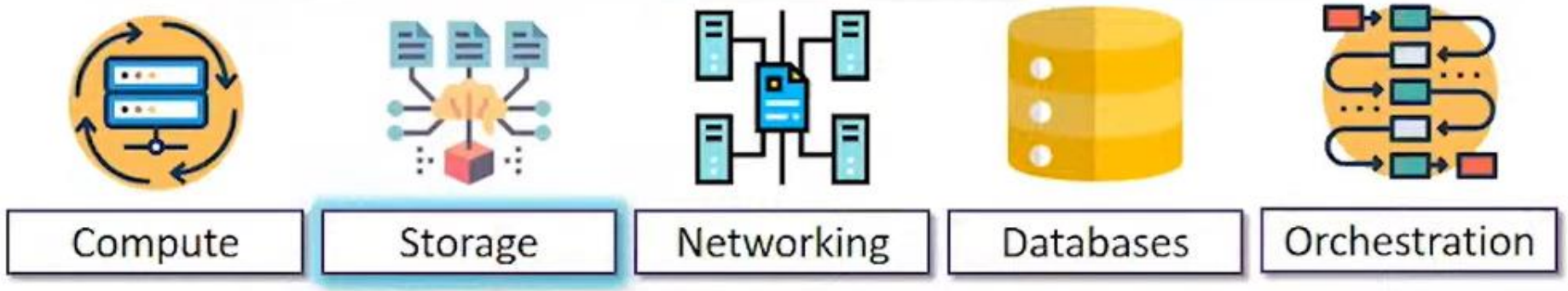
Orchestration

Cloud Building Blocks



- Compute services refer to creation, management and usage of virtual servers which we then use to perform computation tasks
- These servers can then be used by users to offload some resource intensive tasks such as calculations or application deployment etc. e.g. AWS EC2

Cloud Building Blocks

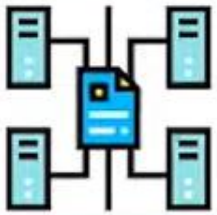


- In cloud computing storage is broken into two categories: Block and Object
- First one is Block storage in which we get a chunk of storage space allocated to us which is then partitioned into drives and managed by operating system e.g. AWS Elastic Block Store
- Second one is Object storage which abstracts the details file storage and management. All these details are handled by your cloud service provider, all we have to do is upload and access files. e.g. AWS S3

Cloud Building Blocks

Compute

Storage



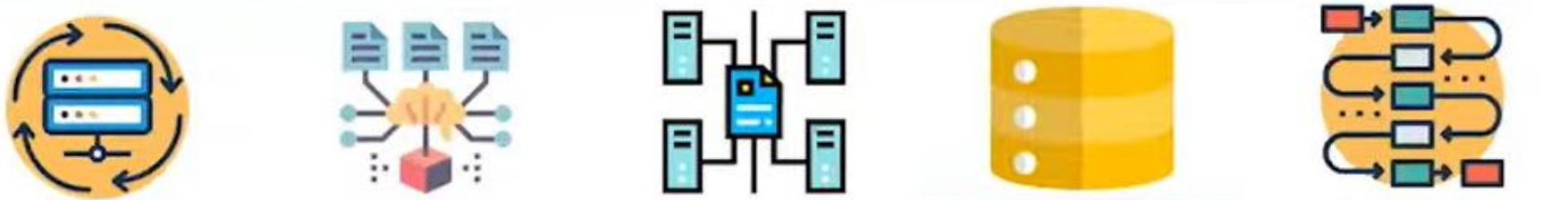
Networking

Databases

Orchestration

- In cloud computing networks allows users to connect several systems together in cloud
- Networks in cloud are highly virtualized to provide high degree of flexibility in designing their networks to suit their own unique business requirements

Cloud Building Blocks



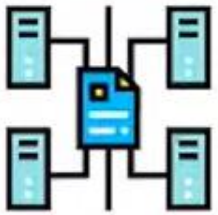
Compute | Storage | Networking | Databases | Orchestration

- In cloud computing users may choose to either build and manage their own database servers on top of existing infrastructure provided by cloud service provider
- However, it is more practical to use a managed database service in which you specify your preferences e.g. database vendor, server capacity, version etc. e.g. AWS RDS
- Managed databases support various kinds of databases which make them more flexible than self managed database servers

Cloud Building Blocks

Compute

Storage



Networking

Databases

Orchestration

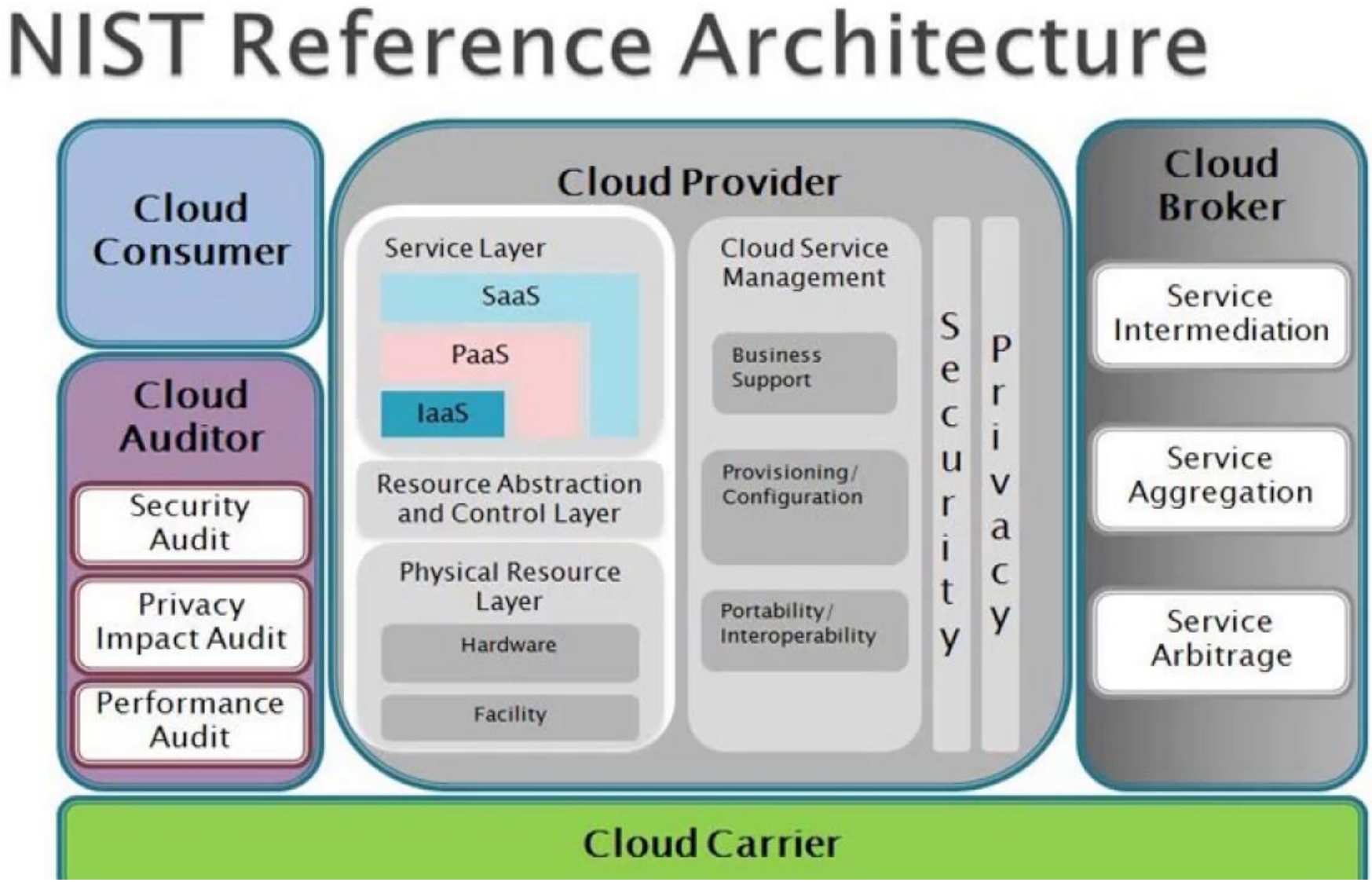
- Spinning Up and managing cloud computing resources manually can get extremely difficult
- Cloud orchestration allows us to create automated workflows for creating and managing cloud environments
- Using cloud orchestration we can quickly and easily create cloud resources, shift operations between environments and perform various other administrative tasks

Cloud Reference Architecture

The International Organization for Standardization publishes a cloud reference architecture in their document, ISO 17789

This document lays out a common terminology framework that assists different parties in communicating about their roles and responsibilities

Cloud reference architecture



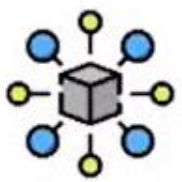
Cloud Computing Activities

There are several activities which are performed in cloud computing, which are broken down into 4 layers, plus a set of functions which spans across the layers. These are:

User Layer

Access Layer

Service Layer



Resource Layer

Multi Layer Functions

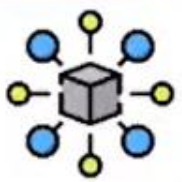
Cloud Computing Activities

The user layer is the user interface through which a customer interacts with cloud services, performs customer related administrative activities, and monitors cloud services

User Layer

Access Layer

Service Layer

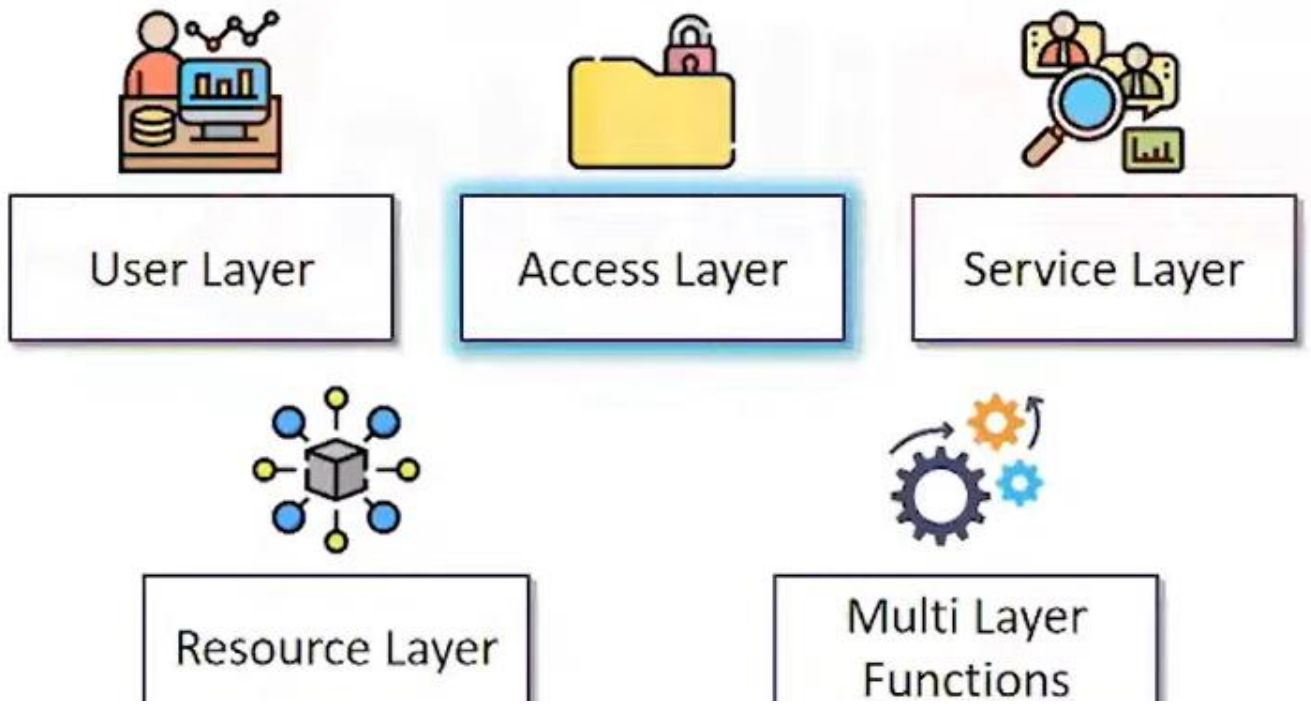


Resource Layer

Multi Layer Functions

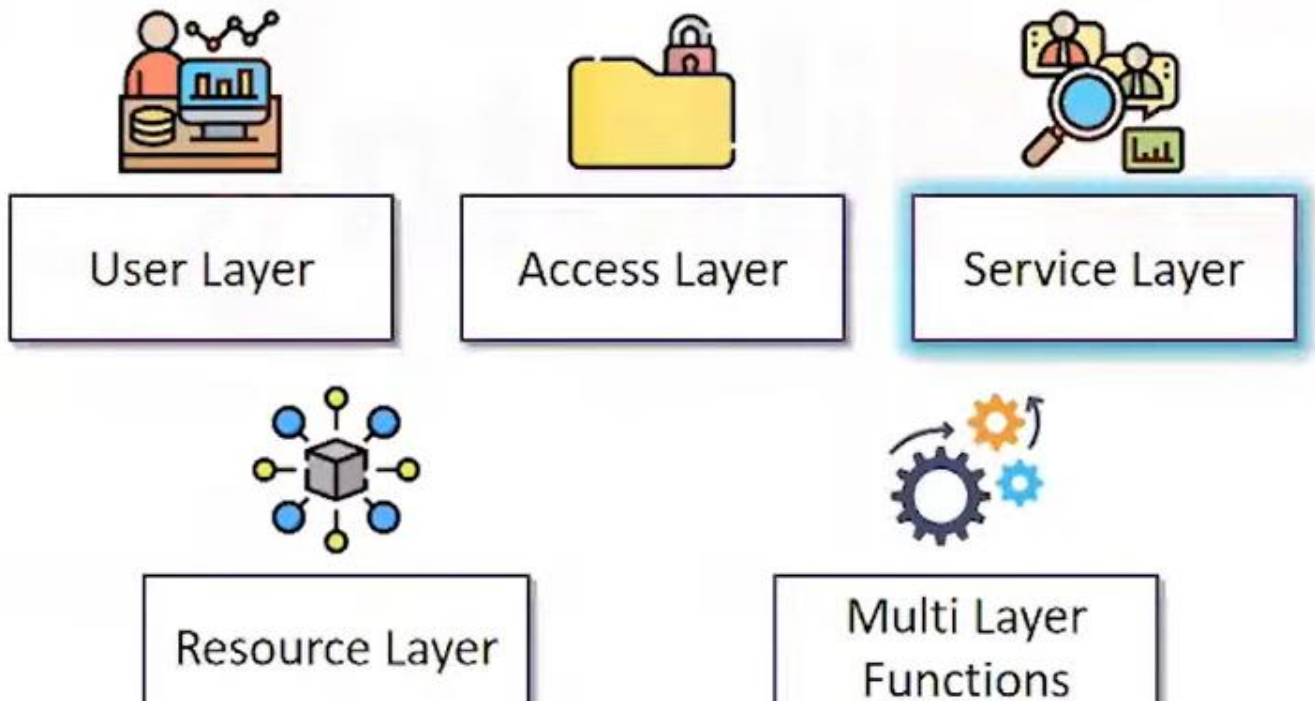
Cloud Computing Activities

The access layer provides a common interface for both manual and automated access to the capabilities available in the services layer



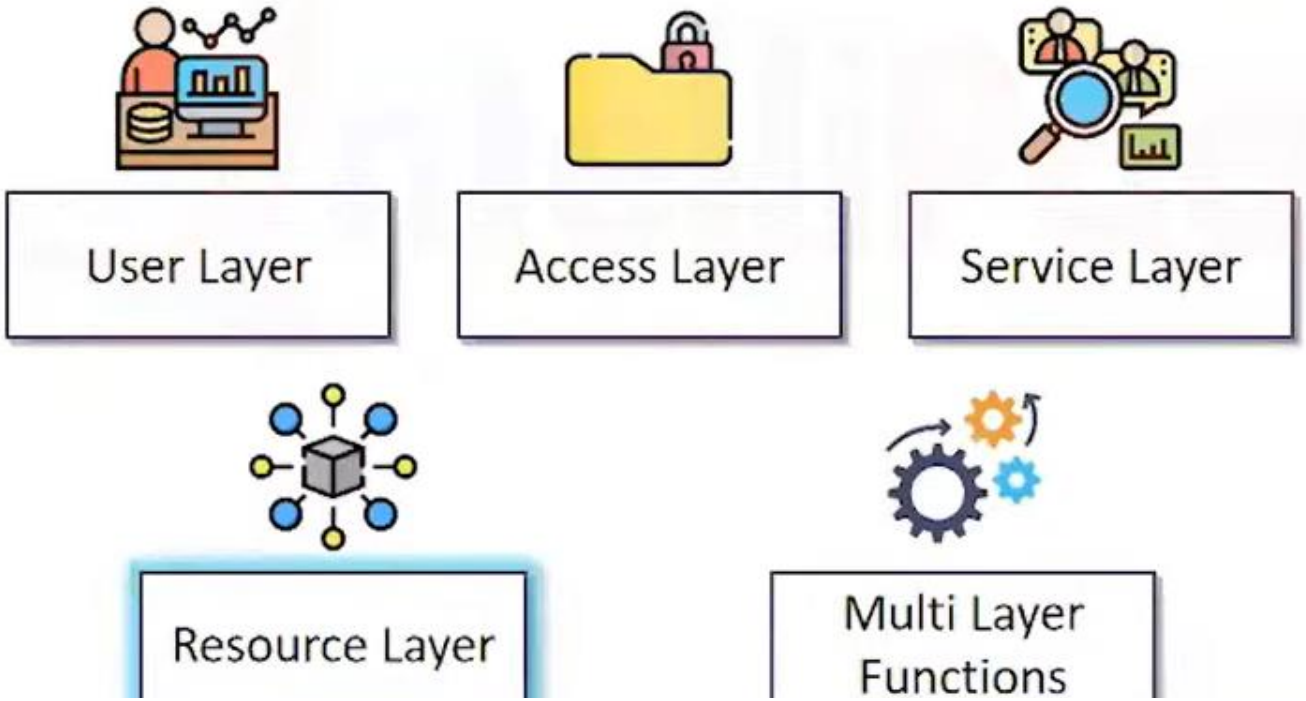
Cloud Computing Activities

The service layer contains the implementation of the services provided by a cloud service provider. The service layer contains and controls the software components that implement the services



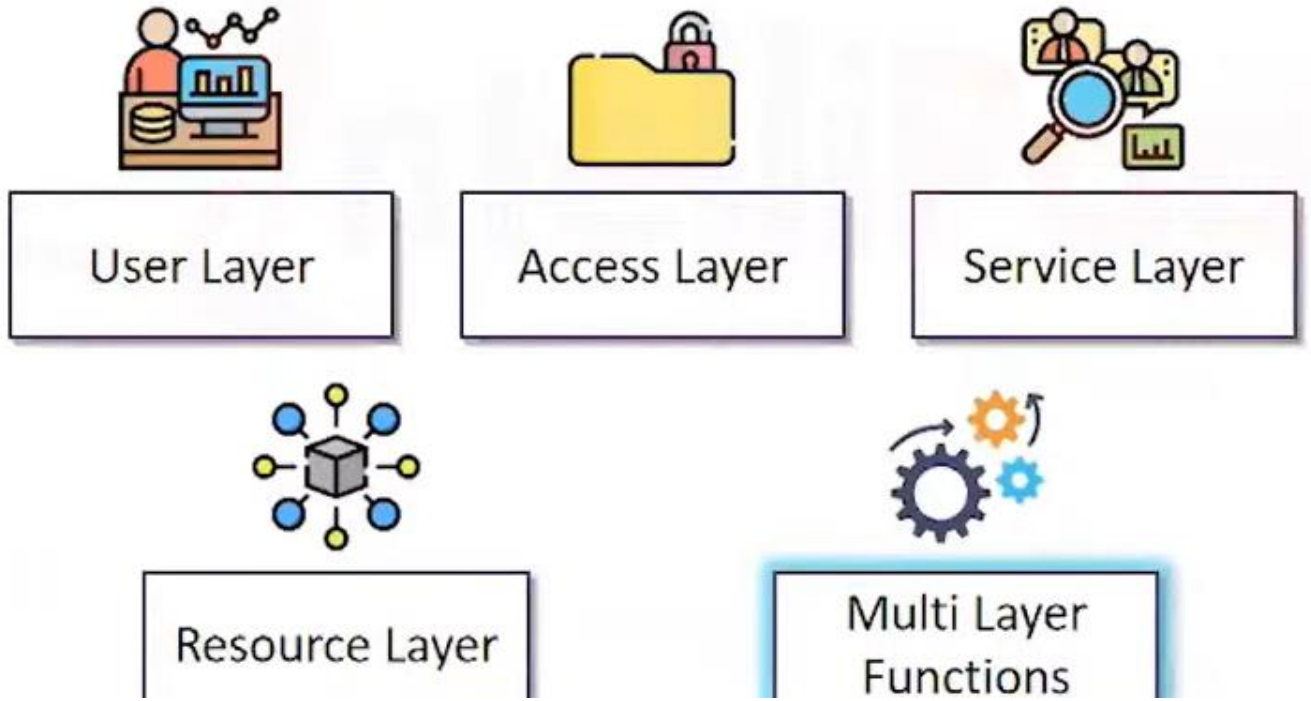
Cloud Computing Activities

The resource layer is where the resources reside. These includes hardware such as servers, networking switches and routers, storage devices, and software that runs on the hardware such as host operating systems, hypervisors, etc.



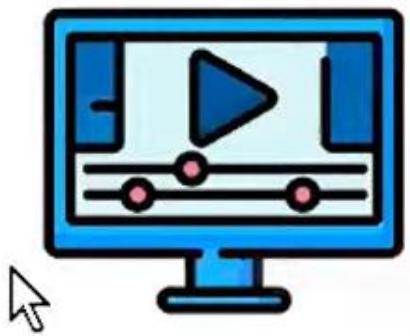
Cloud Computing Activities

Multi Layer functions include functional components that interact with functional components of the above four other layers to provide supporting capabilities such as: integration capabilities, development support capabilities etc.



Cloud Service Capabilities

There are different types of capabilities that we an acquire using cloud services such as:



Application Capability Types

Platform Capability Types

Infrastructure Capability Types

Cloud Service Capabilities

There are several applications that are offered to use by cloud service providers which we use such as - Outlook Mail, Google Drive etc.

Application Capability Types

Platform Capability Types

Infrastructure Capability Types

Cloud Service Capabilities

There are cloud services that offer us pre configured platforms to deploy and manage our own applications e.g. AWS Elastic BeanStalk

Application Capability Types

Platform Capability Types

Infrastructure Capability Types

Cloud Service Capabilities

There are cloud services that offer us basic infrastructure tools such as servers, storage drives etc. which we can configure and use according our own needs

Application Capability Types

Platform Capability Types

Infrastructure Capability Types

Shared Considerations

There are several cross cutting or shared considerations that are addressed in cloud reference architecture. These are:

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

Interoperability is the ability of two or more cloud services to work with each other and exchange information

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

Portability is the ability to move data and operations from one cloud service to another with minimal disruption

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

Reversibility is the extent to which cloud-based applications are designed so that they can be moved to other cloud providers or environments

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

Availability determines how much uptime can be provided by a cloud service

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

Cloud security involves concepts such as: Confidentiality, Integrity and Availability

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Shared Considerations

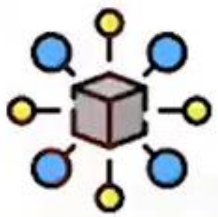
Resiliency is the ability of cloud services to recover from failures and errors

Interoperability	Portability	Reversibility
Availability	Security	Privacy
Resiliency	Performance	Governance
Maintenance	Versioning	Service levels
SLA	Auditability	Regulations

Emerging Technologies

There are several new technologies emerging in the cloud such as:

Machine Learning



Blockchain

IoT

Containers

Quantum Computing

Cloud Computing Security Concepts

There are six key security concepts relevant to cloud computing, these are:

- Cryptography
- Access Control
- Data and Media Sanitization
- Network Security
- Virtualization Security
- Common Threats

Cryptography

In cloud computing cryptography plays a major role in data security. Some important aspects to consider are

- Encryption
- Key Management
- Data In Motion and At Rest

Access Control

Access Control is a major source of security flaws in cloud computing

- Access Control refers to granting and revoking a users authorization over some data or service
- In cloud computing access control can be managed is several ways
- However, in real-world practice, organizations tend to manage access control locally due to its importance to organizational information security
- This is done so that the organization has full control over granting and revoking access to cloud computing services and data

Data and Media Sanitization

Data and Media Sanitization refers to dealing with encrypted data when being erased, changed or overwritten

- When dealing with secure and encrypted data there are several concerns we need to be aware of
- For example we may have to delete or overwrite a small piece of data that is encrypted using a key
- If that key is only used for that data then we should remove the data and then remove the key as well
- For security purposes all cryptographically secured data should be deleted or overwritten in such a way that it cannot be recovered successfully

Network Security

Network Security allows us to impose restrictions on incoming and outgoing traffic in a virtual or real network

- Many cloud services provide several tools which we can use to better protect our virtual networks in the cloud
- For example we can use Network Security Groups for applying specific security rules on a group of resources
- Firewalls should be properly used to prevent unauthorized access to our networks
- Set security rules only to grant networking access to resources that need them i.e. grant minimal required access

Virtualization Security

Virtualization comes with it's own set of security concerns

- As Virtualization deals with hypervisors and host OS as well we need to be cognizant of several flaws in their security
- A Virtual Machine attached to a hypervisor is affected when the 'host' hypervisor is also compromised
- Even when you are using containers you have to be cognizant of these security concerns
- Common Virtualization Security threats include Denial of Service Attack (DoS), Host Traffic Interception, VM Jumping

Common Threats

The Cloud Security Alliance (CSA) has defined nine of the most common security threats in cloud computing, these are:

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Common Threats

In simple terms data breach refers to a situation where the data is accessed by someone who is not supposed to have access to it

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Common Threats

Users may end up losing their personal and valuable data on cloud computing platforms because of various reasons and if no backup is present then the data is permanently lost

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Common Threats

We may expose several APIs to allow integration with customers on premise systems, and therefore, we need to have the proper authentication and authorization mechanism in place

Data Breach	Data Loss	Insecure Interfaces
Account and Service Hijacking	DoS and DDoS attacks	Malicious Insiders
Abuse of Cloud-Based Services	Shared Technology Vulnerabilities	Insufficient Due Diligence

Common Threats

Attack methods such as phishing, fraud, and exploitation are used for gaining access to users credentials and therefore their accounts become compromised

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Common Threats

These attacks prevent legitimate users of a cloud service from gaining access to their data and applications because of system slowdown caused by a large volume of requests coming to these services

Data Breach	Data Loss	Insecure Interfaces
Account and Service Hijacking	DoS and DDoS attacks	Malicious Insiders
Abuse of Cloud-Based Services	Shared Technology Vulnerabilities	Insufficient Due Diligence

Common Threats

A malicious insider is a current or former employee who has or had authorized access to an organization's network, system, or data and intentionally misuses that access to negatively affect its security

Data Breach	Data Loss	Insecure Interfaces
Account and Service Hijacking	DoS and DDoS attacks	Malicious Insiders
Abuse of Cloud-Based Services	Shared Technology Vulnerabilities	Insufficient Due Diligence

Common Threats

A malicious user might end up using cloud services to do some damage to another organizations network such as a DDoS attack, Brute Force attack to guess someone's credentials etc.

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Common Threats

Since cloud providers use virtualization if any host system becomes compromised then multiple virtual systems become compromised as well

Data Breach	Data Loss	Insecure Interfaces
Account and Service Hijacking	DoS and DDoS attacks	Malicious Insiders
Abuse of Cloud-Based Services	Shared Technology Vulnerabilities	Insufficient Due Diligence

Common Threats

If an organization using cloud computing services do not take care of security on their end using techniques such as encryption, security monitoring etc. then an attacker could exploit these loopholes

- Data Breach
- Data Loss
- Insecure Interfaces
- Account and Service Hijacking
- DoS and DDoS attacks
- Malicious Insiders
- Abuse of Cloud-Based Services
- Shared Technology Vulnerabilities
- Insufficient Due Diligence

Secure Cloud Computing Design Principles

There are five key principles relevant to secure cloud computing, these are:

- Cloud Secure Data Lifecycle
- Disaster Recovery (DR) and Business Continuity (BC)
- Cost Benefit Analysis
- Functional Security Requirements
- Cloud Categories Security Considerations

Cloud Secure Data Lifecycle

This is the first stage when data is being created on any cloud platform or service

Create

Store

Use

Share

Archive

Destroy

BCDR planning

In cloud computing two major design concerns with respect to data are Disaster Recovery and Business Continuity

Disaster Recovery

Business Continuity

BCDR planning

It is the plan of action that needs to be implemented when disaster strikes such as loss of data, data integrity violation etc.

Disaster Recovery

Business Continuity

BCDR planning

It is the objective of Disaster Recovery systems is to ensure business continuity and prevent organizations from suffering substantial damage in the form of losses to revenue, reputation, market share etc.

Disaster Recovery

Business Continuity

Cost Benefit Analysis

Cost Benefit Analysis plays an major role in deciding security concerns and their solutions

- Cost Benefit Analysis allows us to compare different platforms on the basis of expenditure needed for a service with the value provided by that service
- Cost has often been called the “key driver” for whether an organization will adopt cloud computing in some capacity
- Different cloud computing solutions provide different services at different prices and they need to be thoroughly examined to choose the best option

Functional Security Requirements

Functional Security Requirements in cloud, these are:

Portability

Interoperability

Vendor lock-in

Cloud Categories Security Considerations

Depending on the service model we can have different security concerns such as:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Cloud Categories Security Considerations

Depending on the service model we can have different security concerns such as:

Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)

- Is data being encrypted when it is transmitted over the network
- Is the application preventing against common attacks such as SQL Injection, XSS etc.
- Are proper measures in place in case of application security being compromised

Cloud Categories Security Considerations

Depending on the service model we can have different security concerns such as:

Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)

- Are we using the latest version of platform services
- Are the software's being used in deployment up to date with latest security patches
- Is the deployment process using latest security standards

Cloud Categories Security Considerations

Depending on the service model we can have different security concerns such as:

Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)

- Are all the networks properly configured
- Are proper backup and replication strategies in place
- Do host machines have the latest OS and security patches installed on them

Evaluating Cloud Service Providers

There are three major ways of evaluating cloud service providers

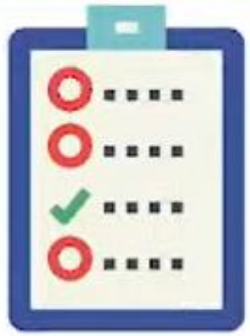
ISO 27017

PCI DSS

Government Security Standards

These are evaluation criteria are for cloud security and compliance, there may be other criteria as well such as price etc.

Evaluating Cloud Service Providers



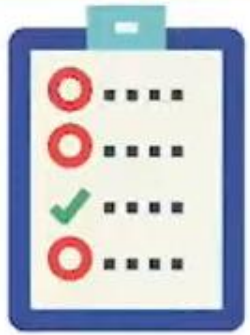
ISO 27017

PCI DSS

Government Security Standards

- It is published by International Organization for Standardization and provides standard guidance for implementing security concerns in the cloud
- Many cloud computing providers offer services that comply with these standards
- If you wish to know which services of which providers are compliant to these services then you can look their offerings and description. E.g. GCP offers several services that comply to the standards

Evaluating Cloud Service Providers



ISO 27017

PCI DSS

Government Security Standards

- It stands for Payment Card Industry Data Security Standard that needs to be adhered by any organizations involved in storage, processing or transmission of credit card information
- If you do handle credit card payments and do not adhere to these standards then a large fine can be levied to you
- This standard is only needed if you are involved in processing credit card payments
- Most services defer to other services for this such as PayPal, Stripe etc.

Evaluating Cloud Service Providers

ISO 27017

PCI DSS

Government Security Standards

- Different Government Agencies are subject to different security standards which need to be adhered to by cloud computing providers
- For example if you are involved in projects dealing with U.S. government then there are several standards you need to adhere to and certifications you need to get
- Common Criteria (CC) Certification for Hardware and Software products and Federal Information Processing Standard (FIPS 140-2) is to certify cryptographic security in government services

Articulate Legal Requirements and Unique Risks

When trying to understand the legal requirements in a cloud environment we need to focus on a few important points. These are:

- Conflicting International Legislation
- Evaluation of Legal Risks Specific to Cloud Computing
- Legal Framework and Guidelines
- eDiscovery
- Forensics Requirements

Conflicting International Legislation

The simplicity of computing and storage provided by the cloud has led to a complexity of legal issues

Below is a list of the possible sources of international legislation conflicts that we must keep in mind when dealing with legal technicalities in cloud:

- Copyright law
- Intellectual property
- Breaches of data protection
- Violation of patents
- Privacy-related components

Evaluation of Legal Risks

Cloud Computing can be subject to several legal risks

There are a huge number of laws and legislative items which may impact cloud environments, such as:

- Legislative law
- State law
- Copyright law
- Piracy law etc

Legal Framework and Guidelines

There are several legal frameworks and guidelines which may help in dealing with legal issues surrounding cloud computing

- Depending on the geographical and judicial location of the users and cloud service infrastructure different legal guidelines may apply
- For instance if your operations are located in European Union then the EU Data Protection Directive may apply.

eDiscovery

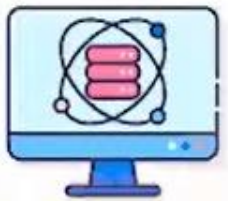
eDiscovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case

- eDiscovery involves the following main steps:

- **Identification:** Data that is potentially relevant to a case is identified, along with its locations, custodians, sizes/volumes etc
- **Preservation:** the identified is placed under a legal hold, starting the formalized forensic process
- **Collection:** Data is collected from the original custodian, typically by physically removing the original digital storage media

Forensics Requirements

For proper cloud security we must understand and accommodate cloud forensic operations. It has several considerations such as:



- Cloud forensics is a subset of digital forensics based on the unique approach to investigating cloud environments.
- Cloud Service Providers have servers around the world to host customer data
- When a cyber incident happens, legal jurisdiction and the laws that govern the region present unique challenges

Country-Specific Legislation of Private Data

Different countries may have different rules and regulations that govern storage and treatment of private data

- Each geographical location may have its own legal rules and regulations for data privacy and protection which needs to be followed by the cloud service providers
- For example the European Union (EU) maintains that the General Data Protection Regulation (GDPR) applies to the personal information of all EU residents wherever they might be located

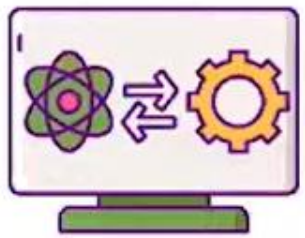
Jurisdictional Differences in Data Privacy

Another thing to keep in mind when dealing with legal rules and regulations that apply on data centers and data stored in them is the jurisdictional rules

- Jurisdiction is the practical authority granted to a legal body to administer justice, as defined by the kind of case, and the location of the issue
- Which is to say the location of the data center may also determine which legal bodies have authority to dictate rules related to the management of private data

Standard Privacy Requirements

Depending on the geographical location there may be several guidelines, regulations, and practices which you may need to follow. Here are three of these which you can take a look at



ISO/IEC 27018

GAPP

GDPR

Standard Privacy Requirements

ISO/IEC 27018

- This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) for the public cloud computing environment
- The objective of this document is to assist the cloud service customer and the public cloud PII (Personally Identifiable Information) processor in entering into a contractual agreement
- The guidelines in this document can also be relevant to organizations acting as

Standard Privacy Requirements

GAPP

- Generally Accepted Privacy Principles (GAPP) is a framework intended to assist Chartered Accountants and Certified Public Accountants in creating an effective privacy program for managing and preventing privacy risks

- The framework was developed through joint consultation between the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) through the AICPA/CICA Privacy Task Force.

Standard Privacy Requirements

GDPR

- The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area
- It also addresses the transfer of personal data outside the EU and EEA areas

Standard Privacy Requirements

GDPR

- The GDPR's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU

- The GDPR 2016 has eleven chapters, concerning general provisions, principles, rights of the data subject, duties of data controllers or processors, transfers of personal data to third countries, supervisory authorities, cooperation among member states, remedies, liability or penalties for breach of rights, and miscellaneous final provisions.

Understand Audit Process, Methodologies etc.

Auditing in cloud computing is very important. There are several aspects to it that we need to understand

Internal and External Audit Controls	Impact of Audit Requirements	Identify Assurance Challenges of Virtualization and Cloud	Types of Audit Reports
Restrictions of Audit Scope Statements	Gap Analysis	Audit Planning	Internal Information Security Management System (ISMS)
Internal Information Security Controls System	Policies	Identification and Involvement of Relevant Stakeholders	Specialized Compliance Requirements for Highly-Regulated Industries
	Impact of Distributed IT Model		

Internal and External Audit Controls

Audits performed by a designated company employee to make sure all operations are following standard practices and logs are being maintained

Internal Audit

External Audit

Impact of Audit Requirements

The nature of cloud computing has made auditors reimagine how they audit

- Auditors now have to worry about several questions such as:
  - What universal population do we sample from?
  - What are the sampling methods for this highly dynamic environment?
  - How to tell if the virtualized server that you are auditing is the same as it was before?

Identify Assurance Challenges of Virtualization

There are 3 main challenges in Service Assurance in the virtualized cloud environments

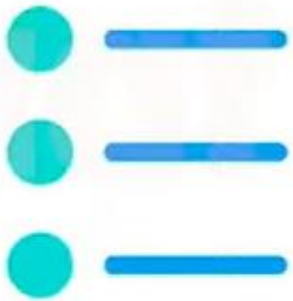
- Ensuring that the data acquired from the networks and its processing happens in real-time
- Building service models that are always completely synchronized with the state of the network
- Converting network/service data into meaningful analytics to serve the business objective

Types of Audit Reports

There are three main types of audit reports that are important for cloud computing audits

SSAE

SOC



ISAE

Types of Audit Reports

SSAE

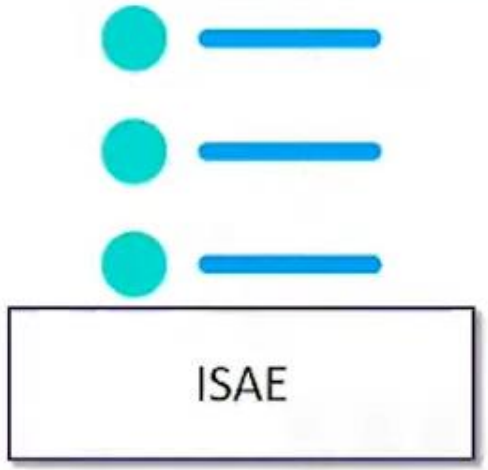
- SSAE stands for Statement on Standards for Attestation Engagements
- It is an auditing standard for service organizations, produced by the American Institute of Certified Public Accountants Auditing Standards Board.
- This standard is used to produce System and Organization Controls (SOC) reports

Types of Audit Reports

SOC

- (SOC) stands for Service Organization Control
- It is a reports that help companies establish trust and confidence in their service delivery processes and controls
- These reports are administered by an independent third party that must be a certified public accountant (CPA)

Types of Audit Reports



- ISAE stands for International Standard on Assurance Engagements
- International Standard on Assurance Engagements is an international assurance standard that prescribes Service Organization Control (SOC) reports, which gives assurance to an organization's customers and service users that the service organization has adequate internal controls

Restrictions of Audit Scope Statements

There are several restrictions of auditing in cloud computing such as:

- **Rely on Experts:** An Auditor has to rely on experts like engineers, values and lawyers for estimation and valuation of fixed assets and estimation of contingent liabilities.
- **Efficiency of Management:** An Auditor does not comment on the efficiency of management working in client organization; no comments on future performance of an organization can be made through audited financial

Gap Analysis

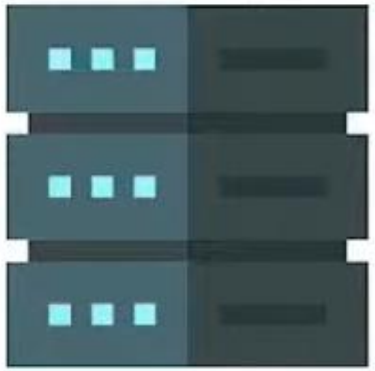
- A gap analysis is a method of assessing the differences in performance between a business' information systems or software applications to determine whether business requirements are being met and, if not, what steps should be taken to ensure they are met successfully

- Gap refers to the space between "where we are" (the present state) and "where we want to be" (the target state)

Audit Planning

- An audit plan is the specific guideline to be followed when conducting an audit
- It helps the auditor obtain sufficient appropriate evidence for the circumstances, helps keep audit costs at a reasonable level, and helps avoid misunderstandings with the client
- The auditor plans to perform the audit in an efficient and timely manner

Internal Information Security Management

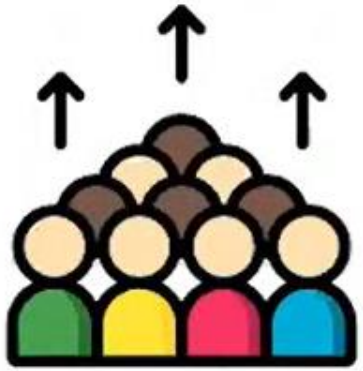


- An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data
- The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach

Policies

- An audit policy defines account limits for a set of users of one or more resources
- It comprises rules that define the limits of a policy and workflows to process violations after they occur
- These policies may be grouped into several levels or groups such as: organizational, functional, cloud computing
- These groups can have different auditing requirements and different auditors as

Identification and Involvement of Stakeholders



- In the auditing process relevant stakeholders should be involved
- These stakeholders must be first identified based on the resources being audited
- After the identification of these stakeholders they should be kept in loop of any relevant updates or information found during the auditing process
- Active Involvement of stakeholders is expected to make the auditing process successful

Specialized Compliance Requirements

- Based on the kind of data being stored, there are times when we have to follow several regulations in storage and retrieval of data
- These regulation may be geographical (i.e. North American Electric Reliability Corporation/ Critical Infrastructure Protection (NERC/CIP)), industry based (Payment Card Industry (PCI)), or sensitivity based as well (Health Insurance Portability and Accountability Act (HIPAA))

Impact of Distributed IT Model

- Since cloud computing is spread across a wide range of geographical locations it further complicates the auditing process
- Based on the geographical locations different laws may apply to the data and infrastructure
- The legal jurisdictions may be vary based on location as well the data being stored on the infrastructure
- Auditors will have to understand the legal and jurisdictional aspects of the infrastructure and data being stored on and proceed accordingly