ST. ANNE'S COLLEGE OF ENGINEERING AND TECHNOLOGY
(Approved by AICTE, New Delhi. Affiliated to Anna University, Chennai)
Accredited by NAAC
ANGUCHETTYPALAYAM, PANRUTI – 607 106.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CSM NOTES

CCS336-CLOUD SERVICE MANAGEMENT

Regulation 2021

PREPARED BY

Ms.K.KAYALVIZHI,AP/CSE

UNIT-I CLOUD SERVICE MANAGEMENT FUNDAMENTALS

Cloud Ecosystem, The Essential Characteristics, Basics of Information Technology Service Management and Cloud Service Management, Service Perspectives, **Cloud Service Models**, **Cloud Service Deployment Models**

PART – A

1. **Define Cloud.**
2. **What is meant by Cloud computing?**
3. **List out the main characteristics of cloud.**
4. **Name the service models available in cloud computing.**
5. **State Deployment model of Cloud Computing.**
6. **Give the advantages of cloud computing.**
7. **What is meant by cloud eco system?**
8. **What are the benefits of ITSM?**
9. **List out the core ITSM processes**.
10. **List out the main actors of the Cloud Ecosystem.**
11. **What are the main features of using continuous delivery?**
12. **What are the advantages of using PaaS?**
13. **What is meant by ITIL?**
14. **What is meant by DEVOPS?**
15. **List out the characteristics of IaaS.**
16. **Differentiate between private cloud and public cloud.**

PART-B:

1. **Explain in detail about the Cloud Ecosystem.**
2. **Describe the Characteristics of Cloud Computing**.
3. **Describe the concepts of perspective in cloud computing.**
4. **Explain in detail about the cloud service model.**
5. **Explain in detail about the deployment model.**

PART-A:

1. **Define Cloud.**

The cloud is a technology that uses remote servers on the internet to store, manage and access data online rather than local drives.

2. **What is meant by Cloud computing?**

Cloud computing refers to the delivery of computing services over the internet, including storage, processing power, and software applications. It allows users to access resources and services on-demand, without the need for physical infrastructure or local servers.

3. **List out the main characteristics of cloud.**

- ✓ On demand self-services
- ✓ Broad Network access
- ✓ Multi tenancy and Resource Pooling
- ✓ Rapid Elasticity
- ✓ Measured Service

4. **Name the service models available in cloud computing.**

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

5. **State Deployment model of Cloud Computing.**

- Public cloud
- Private Cloud
- Hybrid cloud
- Community cloud

6. **Give the advantages of cloud computing.**

- ✓ Improved accessibility
- ✓ Optimum resource utilization
- ✓ Scalability and need
- ✓ Minimizes licencing cost of software
- ✓ Less personnel training

7. **What is meant by cloud eco system?**

A **cloud ecosystem** is a dynamic system of interdependent elements, all of which work together to make cloud services possible. In nature, an ecosystem

consists of objects that are linked and work together that are living and non-living.

8. **What are the benefits of ITSM?**
   - ✓ Aligning IT teams with business priorities through success metrics.
   - ✓ Enabling cross-department collaboration
   - ✓ Empowering IT teams to share knowledge and continuously improve
   - ✓ Improving request coordination for more efficiency service.
   - ✓ Responding more quickly to major incidents, and preventing future ones.

9. **List out the core ITSM processes**.
   - ✓ Service Request Management
   - ✓ Knowledge management
   - ✓ IT asset management
   - ✓ Incident management
   - ✓ Problem Management
   - ✓ Change management

10. **List out the main actors of the Cloud Ecosystem.**

Cloud Service User -Cloud service user (CSU) is an individual or company who uses cloud services that are distributed. End-users may be individuals, machines, or apps.

Cloud service Provider -A company that provides and manages the cloud services provided.

Cloud Service Partner -An entity or organization which supports the creation of the service offer by a partner.

11. **What are the main features of using continuous delivery?**

Visibility: Everyone on the team can see the entire system and collaborate.

Feedback: All team members are notified immediately of any issues.

Continual Deployment: Any version of the software can be deployed to any environment.

12. **What are the advantages of using PaaS**

- Simple, cost-effective development and deployment of apps
- Developers can customize SaaS apps without the headache of maintaining the software
- Provide automation of Business Policy

- Easy migration to the Hybrid Model
- It allows developers to build applications without the overhead of the underlying operating system or cloud infrastructure
- It helps developers to collaborate with other developers on a single app

13. What is meant by ITIL?

ITIL can be abbreviated on Information Technology Infrastructure Library. ITIL is the most widely accepted approach to ITSM. It focuses on practices for aligning IT services with business needs. ITIL can help organizations adapt to ongoing transformation and scale.

14. What is meant by DEVOPS?

DEVOPS is the combination of practices and tools designed to increase an organization's ability to deliver applications and services faster than traditional software development processes.

15. List out the characteristics of IaaS.

- ✓ Resources are available as a service
- ✓ Services are highly scalable
- ✓ Dynamic and flexible
- ✓ GUI and API-based access
- ✓ Automated administrative tasks

16. Differentiate between private cloud and public cloud.

.No	Private Cloud	Public Cloud
1	ivate Clouds tend to cost more than Public Clouds for reserving/constructing the data center.	blic Clouds tend to cost less than Private Clouds, as you use pre-made data centers.
2	onnection is possible only via a private network, which makes them extremely secure	onnection is open on the internet, making them more vulnerable and less secure.
3	ery high performance because of private networks	rformance is moderate
4 5	eliability is very high edicated Servers	Moderate Reliability edicated Servers

PART -B

1. Explain in detail about the Cloud Ecosystem.

A **cloud ecosystem** is a dynamic system of interdependent elements, all of which work together to make cloud services possible.

In nature, an ecosystem consists of objects that are linked and work together that are living and non-living.

The ecosystem consists of hardware and software in cloud computing, as well as cloud clients, cloud developers, consultants, integrators, and collaborators.

Cloud ecosystem working model:

A public cloud provider is the nucleus of a cloud environment. It may be an IaaS provider like Amazon Web Services (AWS) or a vendor like Salesforce for SaaS. Tech companies that use the anchor platform of the provider, as well as consultants and companies that have formed strategic partnerships with the anchor provider are radiating out from the centre of the cloud. Salesforce runs a variety of its services on the infrastructure of AWS, and Salesforce clients can access parts of AWS, such as its Simple Storage Service, through devices called connectors.

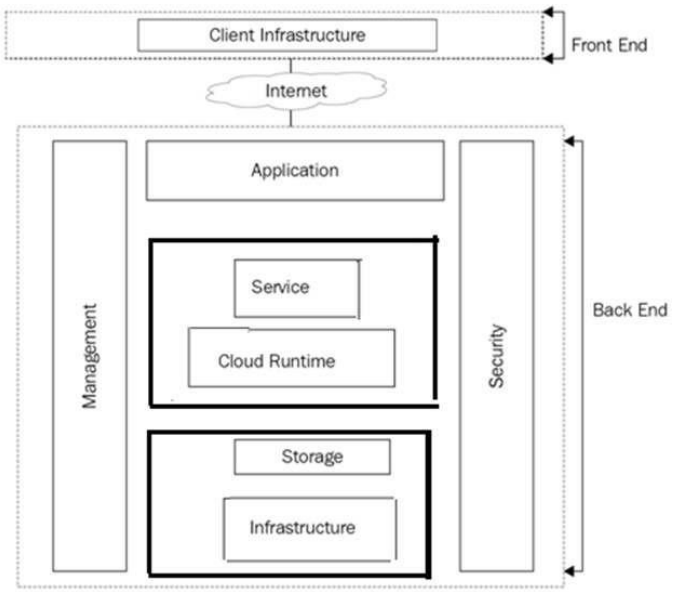
Benefits of a cloud ecosystem:

Aggregating data and evaluating how each component of the system influences the other component is often easier to aggregate.

- **Cloud readiness evaluation** - evaluating the skills to handle and organize the implementation of cloud-enabled solutions
- The vision of **cloud adoption**, outlining our governance plan, planned market performance, and business cases that highlight projected advantages. To construct a step-by-step plan to frame the cloud expedition in an ideal sequence.
- **Use cases** building a set of case studies and scenarios to guide the analysis, selection and prioritization of candidate workloads "cloud-friendly
- **Architectural considerations** - evaluating the architecture of knowledge (data, structure and deployment standards) and application architecture (applications, structure and development standards).

The architecture of the Cloud Ecosystem

The following figure shows the cloud ecosystem architecture.



The main actors of the Cloud Ecosystem are as follows -

Cloud Service User:

- Cloud service user (CSU) is an individual or company who uses cloud services that are distributed.
- End-users may be individuals, machines, or apps.

Cloud service Provider:

- A company that provides and manages the cloud services provided.

Cloud Service Partner:

- An entity or organization which supports the creation of the service offer by a partner.

Cloud computing is one of the most used in information technology. The delivery of IT resources in response to user demand is referred to as cloud computing.

2. Describe the Characteristics of Cloud Computing.

i) **On-Demand Self-Service**:

Cloud computing allows on-demand self-services. Services include storage, networking, analysis, etc. Users can select and use single or multiple services depending on their needs. Users become more accountable for their intake, which improves their ability to make wise decisions. Users can make use of resources following their needs and specifications. They are charged at the end of the billing cycle based on how much they use the services provided by the cloud service providers.

ii) Broad Network Access:

The cloud is accessible to any device from any location because of widespread network access. A cloud provider must offer its clients numerous network access options. Otherwise, a few systems would be available for using the cloud service.

Broad network access contains configuration for secure remote access, paying special attention to mobile cloud computing, regulating the data that broad access network providers have collected, enforcing role-based access control, etc. As a result, cloud computing removes obstacles and borders because it operates across numerous regions.

iii) **Scalability or Rapid Elasticity**:

A system's capacity to manage an increasing volume of work by adding resources is known as scalability. Cloud services must quickly develop to keep up with the ongoing expansion of businesses. One of the most flexible aspects of cloud computing is scalability. In addition to having the potential to increase the number of servers or infrastructure in response to demand, it also offers a significant number of features that satisfy the needs of its clients.

iv) Resource Pooling:

- Resource pooling is one of the core components of cloud computing. A cloud service provider can provide each client with different services based on their demands by employing resource pooling to divide resources across many clients.
- Resource pooling is a multi-client approach for location independence, network infrastructure pooling, storage systems, etc. The process of real-time resource assignment does not affect the client's experience. This is often used in wireless technologies like a radio transmission.

v) Measured Service:

- Cloud systems automatically manage and manage resource utilization by using a metering capability. The consumption of resources is tracked for each application and tenant; it will give both the user and the resource supplier an account of what has been utilized. Monitoring, regulating, and reporting resource utilization allows for transparency for the service provider and the service user.
- The metering capability is built into some level of service abstraction, which enables transparency between the customer and the service provider. Each user

must be billed according to how much of the service they use, and the cloud provider must be able to measure this usage.

vi) **Security**:

- Users of cloud computing are particularly concerned about data security. Cloud service providers store users' encrypted data and offer additional security features like user authentication and protection against breaches and other threats.
- User authentication entails identifying and verifying a user's authorization. Access is denied to the user if they do not have permission. Data servers are physically protected. These servers are usually kept in a secure, isolated location to prevent unauthorized access or disruption.

vii) **Automation**:

- Automation in cloud computing refers to a cloud service's ability to be installed, configured, and maintained automatically. In other words, it is the process of maximizing technology and minimizing the amount of manual labor necessary. However, it is not simple to automate the cloud ecosystem. It requires the deployment of significant storage, servers, and virtual machines. After successful deployment, these resources need to be maintained.

viii) **Budget Friendly**:

- Businesses can reduce their IT expenses by utilizing this aspect of the cloud. In cloud computing, the client is responsible for paying the administration for any space they use. There are no additional fees or hidden costs to be paid.

ix) **Flexibility**:

- Cloud computing users can access data or services with internet-enabled devices like smartphones and laptops. You can instantly access anything you want in the cloud with just a click, making working with data and sharing it simple.
- Many businesses prefer to store their work on cloud systems because it facilitates collaboration and saves money and resources. Its expansion is also being sped up by the number of features analytic tools offer.

X) **Resilience**:

- Resilience in cloud computing refers to a service's capacity to quickly recover from any disruption. The speed at which a cloud's servers, databases, and network system restart and recover from damage or harm is a measure of its resilience.

3. Describe the concepts of perspective in cloud computing.

In today's world of computing, everybody is a decision-maker (or at least they should be). We will first look at cloud computing from the perspectives of various IT Professionals and then we will pass through the DevOps pipeline to explore different cloud considerations along the way.

Developers:

Development environments have changed to accommodate the migration from monolithic application deployment on a server, to microservices provisioned onto some distributed cloud environment in an automated way. Historically we have created sandbox environments for testing, and have made extreme efforts to create identical conditions in all stages of deployment (i.e. development, testing, staging, and production) down to the hardware.

Operations Professionals:

Automation is needed to make the environments we deploy code in as predictable as possible. Gone are the days of administrators and engineers who perform manual one-off tasks to stand up an environment. Orchestration has become the norm as we complete the pipeline from version control to production release.

Network Engineers:

By separating network traffic into control plane (routing/networking information) and data plane (payload/application traffic) Even though these software switches run on hardware switches, there is an element of programming that has been introduced into the daily life of many network professionals.

Project Managers:

Most organizations that develop software now have SCRUM Masters, instead of Project Managers (PM), who serve on a SCRUM Team and represent their team and their efforts to stakeholders. Accountability has become a daily event, and team members celebrate failure and success equally, as they version-up their software with every feature for all to see and test. In the past, the PM would likely blame somebody for not getting some task done on time for a project milestone, but now the culture has completely changed. SCRUM Masters use tools to manage SCRUM related activities, rather than Gantt charts (used for project scheduling) for larger milestones with dependent tasks.

End Users :

The availability of services and the lack of downtime are the biggest advantages of choosing to use applications built on cloud systems. For many consumers, these may not be important considerations, but for organizations, it is imperative to ensure the

availability of services. The SCRUM Team works very hard to anticipate what a user's experience will be and base all of their efforts off from this projection known to them as a "user story."

Version Control:

When version control is employed, not only is code made available throughout an organization with proper access controls, but every change is recorded and accessible. Prior to cloud-hosted version control, thousands of hours of work and code have been lost (either buried in a project as commented lines or deleted entirely).

Continuous Integration(CI):

The first step down the pipeline is the 'build server' that takes every version of the code in the version-controlled source code repository to run preliminary tests. This will ensure that the code does not negatively affect code submitted by other developers.

Continuous Delivery (CD):

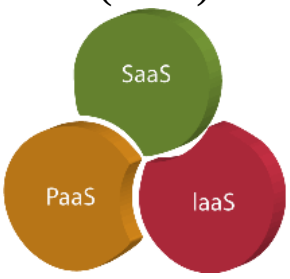
After the software is built and all of the automated tests are successful the code is made available for user acceptance testing (UAT). At the heart of CD is automation. The main features provided by a CD solution are:

- Visibility: Everyone on the team can see the entire system and collaborate.
- Feedback: All team members are notified immediately of any issues.
- Continual Deployment: Any version of the software can be deployed to any environment.

4. Explain in detail about the cloud service model.

There are the following three types of cloud service models -

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)



Infrastructure as a Service (IaaS):

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS:

There are the following characteristics of IaaS -

- ✓ Resources are available as a service
- ✓ Services are highly scalable
- ✓ Dynamic and flexible
- ✓ GUI and API-based access
- ✓ Automated administrative tasks

Example: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

Advantages of IaaS:

- Easy to automate the deployment of storage, networking, and servers.
- Hardware purchases can be based on consumption.
- Clients keep complete control of their underlying infrastructure.
- The provider can deploy the resources to a customer's environment anytime.
- It can be scaled up or downsized according to your needs.

Disadvantages of IaaS:

- You should ensure that your apps and operating systems are working correctly and providing the utmost security.
- You're in charge of the data, so if any of it is lost, it's up to you to recover it.
- IaaS firms only provide the servers and API, so you must configure everything else.

Platform as a Service (PaaS):

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS:

There are the following characteristics of PaaS -

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

Advantages PaaS:

- Simple, cost-effective development and deployment of apps
- Developers can customize SaaS apps without the headache of maintaining the software
- Provide automation of Business Policy
- Easy migration to the Hybrid Model
- It allows developers to build applications without the overhead of the underlying operating system or cloud infrastructure
- Offers freedom to developers to focus on the application's design while the platform takes care of the language and the database
- It helps developers to collaborate with other developers on a single app

Disadvantages of PaaS:

Less flexibility and control
Price
Vendor lock-in
Security
Integration issues

Software as a Service (SaaS):

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS:

There are the following characteristics of SaaS -

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.
- The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting.

Advantages SaaS:

- The biggest benefit of using SaaS is that it is easy to set up, so you can start using it instantly.
- Compared with on-premises software, it is more cost-effective.

- You don’t need to manage or upgrade the software, as it is typically included in a SaaS subscription or purchase.
- It won’t use your local resources, such as the hard disk typically required to install desktop software.
- It is a cloud computing service category that provides a wide range of hosted capabilities and services.
- Developers can easily build and deploy web-based software applications.
- You can easily access it through a browser.

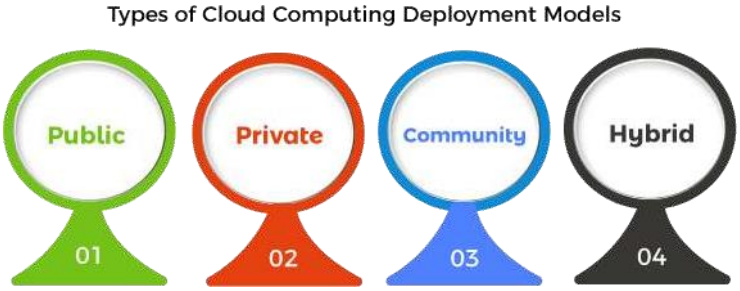
Disadvantages SaaS:

- ✓ Lack of control
- ✓ Security and data concerns
- ✓ Limited range of applications
- ✓ Connectivity requirement
- ✓ Performance

5. Explain in detail about the deployment model.

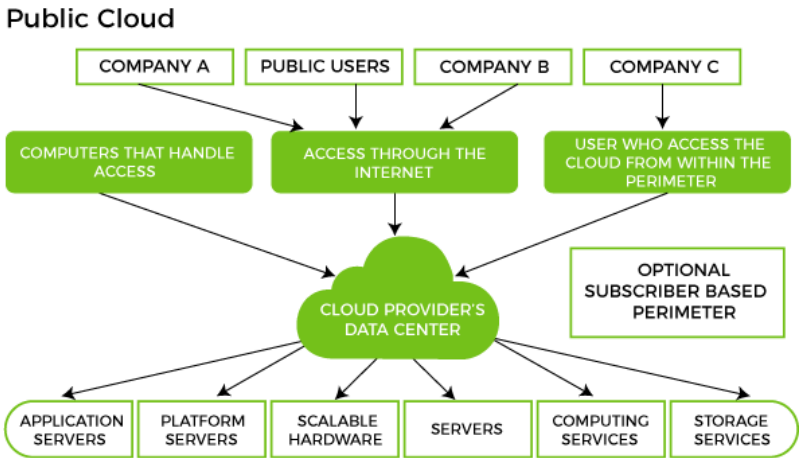
Different Types of Cloud Computing Deployment Models

Most cloud hubs have tens of thousands of servers and storage devices to enable fast loading.



Public Cloud:

It is accessible to the public. Public deployment models in the cloud are perfect for organizations with growing and fluctuating demands. It also makes a great choice for companies with low-security concerns. It is also a great delivery model for the teams with development and testing. Its configuration and deployment are quick and easy, making it an ideal choice for test environments.



Benefits of Public Cloud:

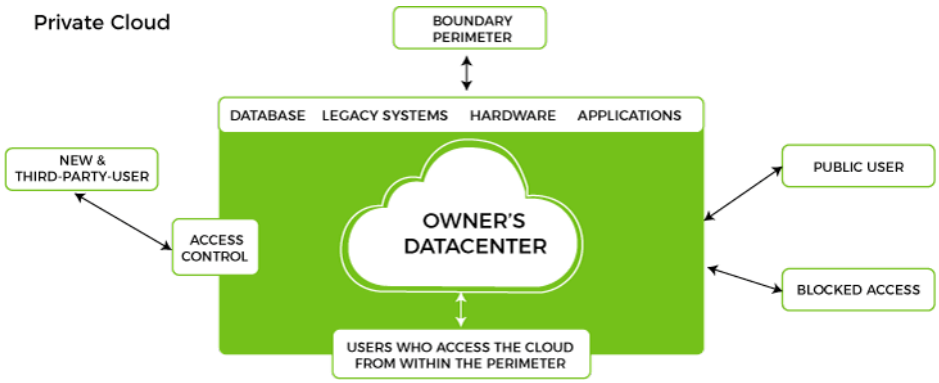
- **Minimal Investment** - As a pay-per-use service, there is no large upfront cost and is ideal for businesses who need quick access to resources
- **No Hardware Setup** - The cloud service providers fully fund the entire Infrastructure
- **No Infrastructure Management -** This does not require an in-house team to utilize the public cloud.

Limitations of Public Cloud:

- **Data Security and Privacy Concerns** - Since it is accessible to all, it does not fully protect against cyber-attacks and could lead to vulnerabilities.
- **Reliability Issues** - Since the same server network is open to a wide range of users, it can lead to malfunction and outages
- **Service/License Limitation** - While there are many resources you can exchange with tenants, there is a usage cap.

Private Cloud:

It means that it will be integrated with your data center and managed by your IT team. Alternatively, you can also choose to host it externally. The private cloud offers bigger opportunities that help meet specific organizations' requirements when it comes to customization. It's also a wise choice for mission-critical processes that may have frequently changing requirements.



Benefits of Private Cloud:

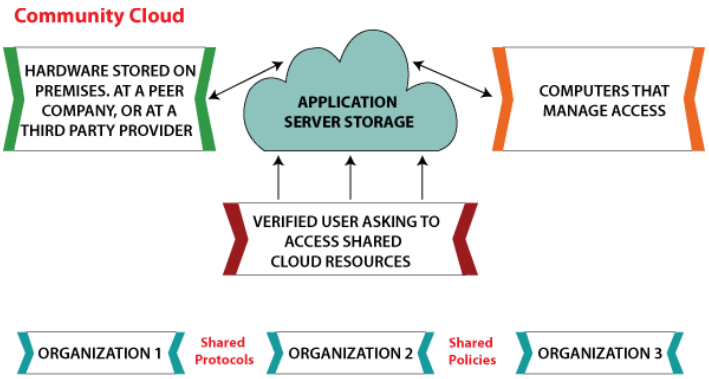
- **Data Privacy** - It is ideal for storing corporate data where only authorized personnel gets access
- **Security** - Segmentation of resources within the same Infrastructure can help with better access and higher levels of security.
- **Supports Legacy Systems** - This model supports legacy systems that cannot access the public cloud.

Limitations of Private Cloud:

- **Higher Cost** - With the benefits you get, the investment will also be larger than the public cloud. Here, you will pay for software, hardware, and resources for staff and training.
- **Fixed Scalability** - The hardware you choose will accordingly help you scale in a certain direction
- **High Maintenance** - Since it is managed in-house, the maintenance costs also increase.

Community Cloud:

The community cloud operates in a way that is similar to the public cloud. There's just one difference - it allows access to only a specific set of users who share common objectives and use cases. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor. However, you can also choose a combination of all three.



Benefits of Community Cloud:

- **Smaller Investment** - A community cloud is much cheaper than the private & public cloud and provides great performance
- **Setup Benefits** - The protocols and configuration of a community cloud must align with industry standards, allowing customers to work much more efficiently.

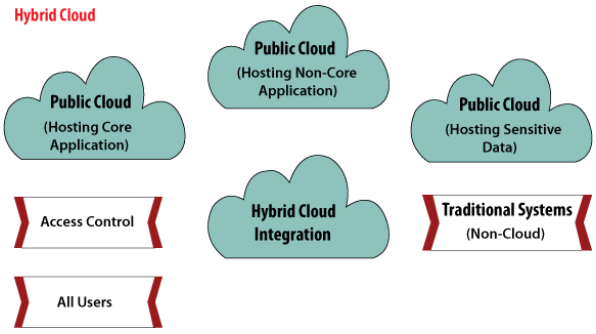
Limitations of Community Cloud:

- **Shared Resources** - Due to restricted bandwidth and storage capacity, community resources often pose challenges.
- **Not as Popular** - Since this is a recently introduced model, it is not that popular or available across industries

Hybrid Cloud:

A hybrid cloud is a combination of two or more cloud architectures. While each model in the hybrid cloud functions differently, it is all part of the same architecture. Further, as part of this deployment of the cloud computing model, the internal or external providers can offer resources.

For Example, a company with critical data will prefer storing on a private cloud, while less sensitive data can be stored on a public cloud. The hybrid cloud is also frequently used for 'cloud bursting'. It means, supposes an organization runs an application on-premises, but due to heavy load, it can burst into the public cloud.



Benefits of Hybrid Cloud:

- **Cost-Effectiveness** - The overall cost of a hybrid solution decreases since it majorly uses the public cloud to store data.
- **Security** - Since data is properly segmented, the chances of data theft from attackers are significantly reduced.
- **Flexibility** - With higher levels of flexibility, businesses can create custom solutions that fit their exact requirements

Limitations of Hybrid Cloud:

- **Complexity** - It is complex setting up a hybrid cloud since it needs to integrate two or more cloud architectures
- **Specific Use Case** - This model makes more sense for organizations that have multiple use cases or need to separate critical and sensitive data

A Comparative Analysis of Cloud Deployment Models:

With the below table, we have attempted to analyze the key models with an overview of what each one can do for you:

Important Factors to Consider	**Public**	**Private**	**Community**	**Hybrid**
Setup and ease of use	Easy	Requires professional IT Team	Requires professional IT Team	Requires professional IT Team
Data Security and Privacy	Low	High	Very High	High
Scalability and flexibility	High	High	Fixed requirements	High
Cost-Effectiveness	Most affordable	Most expensive	Cost is distributed among members	Cheaper than private but more expensive than public
Reliability	Low	High	Higher	High

UNIT-II-CLOUD SERVICES STRATEGY

Cloud Strategy Fundamentals, Cloud Strategy Management Framework, **Cloud Policy**, Key Driver for Adoption, **Risk Management**, IT Capacity and Utilization, Demand and Capacity matching, Demand Queueing, **Change Management**, **Cloud Service Architecture**

PART-A:

1. What are the main phases of strategic plan in cloud computing?
2. List out the strategic life cycle in cloud computing.
3. What is meant by cloud policy?
4. Define Risk management.
5. List out the process of Risk Management.
6. Why we Need for Risk Management?
7. What is meant by Queueing Theory?
8. Define Change Management.
9. List out types of Risks in Cloud Computing:
10. List out the steps for planning.
11. Give the objectives of demand queuing.
12. What are the characteristics of cloud service capacity planning?
13. Differentiate demand and capacity matching**.**

PART-B

1. Explain in detail about the Cloud strategy.
2. Describe the concepts of Cloud Policy.
3. Explain the various concepts of Risk Management.
4. Explain in detail about the Queuing theory in Cloud System Management.
5. Explain in detail about the Change Management:
6. Describe the cloud service architecture**.**

PART-A:

1. **What are the main phases of strategic plan in cloud computing?**
   - ✓ Strategy Phase
   - ✓ Planning Phase
   - ✓ Deployment Phase

2. **List out the strategic life cycle in cloud computing.**
   - ✓ Planning for utilizing cloud technology
   - ✓ Capabilities of an enterprise
   - ✓ Target architecture require
   - ✓ Transition planning & gap analysis
   - ✓ Planning to implement cloud
   - ✓ Governance & significance of SOA (Service-Oriented Architecture)

3. **What is meant by cloud policy?**

   Cloud policies are the guidelines under which companies operate in the cloud. cloud policies can also be used for financial management, cost optimization, performance management, and network security.

4. **Define Risk management.**

   Risk management is the process of identifying, assessing, and controlling threats to an organisation's system security, capital and resources. Effective risk management means attempting to control future outcomes proactively rather than reactively

5. **List out the process of Risk Management.**
   - ✓ Identify the risk
   - ✓ Analyze the risk
   - ✓ Evaluate the risk
   - ✓ Treat the risk
   - ✓ Monitor or Review the risk

6. **Why we Need for Risk Management:**

These risks need to be treated proactively by implementing risk management strategies. By implementing a risk management plan and considering the various potential risks or events before they occur, an organisation may save money and time and protect its future. In cloud computing, the organisation sets risk management plans which help them to identify

appropriate cloud vendors and service providers, make proper service-level agreements and set up better budgeting plans.

7. What do you meant by Queueing Theory?

The queuing system in cloud service system consist of input source i.e. source of requests, queuing process which has waiting requests in the queue to be served, service process which comprises of servers to process the various requests in the queue

8. Define Change Management.

Change management is a continuous process and delivers value to an organization only if deals with agility. Cloud change management allows change leaders to anticipate and accommodate the upcoming change for better preparedness and reduced downtime.

9. **List out types of Risks in Cloud Computing:**

- ✓ Data Breach
- ✓ Cloud Vendor Security Risk
- ✓ Availability
- ✓ Compliance

10. List out the steps for planning.

- ✓ Development of Business Architecture
- ✓ Development of IT Architecture
- ✓ QOS development requirement
- ✓ Development of Transformation plan

11. Give the objectives of demand queuing.

Queue management's main focus is on **customer experience**, but the value of a queue system is not limited to solving queues. Queue management helps decrease customer wait and service times, improve service and staff efficiency, thereby increasing revenue.

12. What are the characteristics of cloud service capacity planning?

Capacity planning **seeks to match demand to available resources**. Capacity planning examines what systems are in place, measures their performance, and determines patterns in usage that enables the planner to predict demand. Resources are provisioned and allocated to meet demand.

13. Differentiate demand and capacity matching.

Capacity refers to the level of output that a company can produce over a certain time period. When the demand for a company's product falls below the

capacity, it can result in a company producing more inventory than it requires. If the demand exceeds capacity, it may lead to a shortage of resources.

PART-B

1. **Explain in detail about the Cloud strategy.**

There is no inadequacy of Cloud Computing technology-based services of users are financially ready. Cloud is considered as the most cheapest, faster and easy-to-use technology and is undoubtedly considered as the rescuer for almost every business these days. With the constantly increasing cost of data storage solutions, it's getting tough for the business holders of small as well as large-scale enterprises to invest.

Users must consider the following the issues:

- Client accessing facility
- Budget requirement
- Type of deployment - private, public, community or hybrid
- Privacy and Data security
- Data backup requirement
- Data export requirement
- Requirement of training

The three main phases are:

1. Strategy Phase
2. Planning Phase
3. Deployment Phase

Strategy phase:

There are two steps of examining this phase:

- Value proposition of Cloud technology: It involves IT management simplifications, maintaining cost reduction, low-cost outsourcing, high QoS (quality of service) outsourcing & innovation in the business model.
- Strategy planning of Cloud technology: Based on analysis of value proposition, the strategy is established; and the strategy documentation is made according to the problems the customer might encounter while using cloud technology.

Planning Phase:

Here the problem analysis & risk analysis for switching to cloud technology is checked to ensure whether the customer is satisfied in meeting their business goals or not.

The steps for planning are:

- **Development of Business Architecture**
- **Development of IT Architecture**
- **QOS development requirement**
- **Development of Transformation plan**

Deployment Phase:

Deployment Phase pivots its strategies based on the above two phases of planning and involves the following steps:

- **Selecting appropriate providers of Cloud:** This selection is made based on SLA (Service Level Agreement), which defines the level of service the cloud-provider will provide.
- **Maintaining the Technical Service:** The provider must ensure the proper maintenance of services by providing the best Quality of Service to their users.

Factors to Be Consider Before Investing in Cloud:

Many IT firms and companies want to revolutionize their infrastructure & technology; Cloud computing became a boon for them. It is undeniable that cloud technology changed the modern scenario of technology, but it is also a truth that there are certain concerns (such as: security, fast internet connection etc) that shows its drawbacks. So as users who will invest their money on cloud technology, they have to consider every aspect thoroughly.

The factors are:

- **Availability:** As soon as all your business-critical data get stored in the cloud storage, it becomes essential to check whether the data is available or not, whether the data is secured or there are loopholes that might become the reason of the downfall of an organization's business. Therefore, as a user you should stay focus & check this aspect with the service provider before signing the deal.
- **Compliance:** Even though it seems that all data gets stored in the cloud storage, but data resides on multiple servers; these servers are located in different nations of the globe. Though it has an advantage for data availability, users must concern about the legality issue; the issue in the sense

- users need to check whether there will be any discrimination or restriction for a particular type of data to store beyond national boundaries.

- **Compatibility:** Users must check the compatibility of IT infrastructure of his/her organization before investing money in Cloud. Though cloud technology is providing users with the optimum possible benefits, as a vendor users must also harvest and extract the maximum usage of cloud. Moreover, it has to keep in mind that the employees of the organization must cope-up with the infrastructure of the cloud technology.
- **Monitoring:** As you put your data on cloud storage, the cloud service provider takes the responsibility and control of your data. For this reason, monitoring becomes an issue. Since complete monitoring of data is possible, so users should make sure that proper monitoring of data is allowed by the providers based on user requirement.

The cloud technology adaptation strategy includes the following:

1. Planning for utilizing cloud technology
2. Capabilities of an enterprise
3. Target architecture require
4. Transition planning & gap analysis
5. Planning to implement cloud
6. Governance & significance of SOA (Service-Oriented Architecture)

2. Describe the concepts of Cloud Policy.

Cloud Policy:

Cloud policies are the guidelines under which companies operate in the cloud. cloud policies can also be used for financial management, cost optimization, performance management, and network security.

Cloud computing offers companies a number of advantages including low costs, high performance, and the quick delivery of services. However, without the implementation and enforcement of cloud policies, companies can be exposed to the risks of data loss, spiraling costs, and underperforming assets.

Cloud Computing Policy

This policy applies to all persons accessing and using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by Loyola University Chicago, all consultants or agents of Loyola University Chicago and any parties who are contractually bound to handle data

produced by Loyola, and in accordance with University contractual agreements and obligations.

The purpose of this policy is to ensure that Loyola Protected or Loyola Sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, Loyola University Chicago for services such as, but not limited to, social networking applications (i.e. all social media, blogs and wikis), file storage (See Listing of Cloud Storage Services in Appendix), and content hosting (publishers text book add-ons). Acceptable and unacceptable cloud storage services are listed in the appendix. All other cloud services are approved on a case by case basis.

REASON FOR POLICY

This policy endorses the use of cloud services for file storing and sharing

1) with vendors who can provide appropriate levels of protection and recovery for University information.

2) with explicit restrictions on storage of University Protected Information.

While cloud storage of files can expedite collaboration, and sharing of information anytime, anywhere, and with anyone, there are some guidelines that should be in place for the kind and type of university information that is appropriate for storing and sharing using these services. Even with personal use, one should be aware of the level of protection available for your data using such a cloud service.

Federal and State laws and regulations place a premium on institutions' ability to understand the risks of IT services and systems and make appropriate determinations about risk tolerance. Some cloud providers, for instance, might mine data for marketing purposes.

There are a number of information security and data privacy concerns about use of cloud computing services at the University. They include:

- University no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws Loss of privacy of data, potentially due to aggregation with data from other cloud consumers.
- University dependency on a third party for critical infrastructure and data handling processes

- Potential security and technological defects in the infrastructure provided by a cloud vendor.
- University has limited-service level agreements for a vendor's services and the third parties that a cloud vendor might contract with
- University is reliant on vendor's services for the security of some academic and administrative computing infrastructure.

POLICY

The following table outlines the data classification and proper handling of Loyola data.

Data Classification	Cloud Storage (See appendix for approved services)	Network Drive *(LUC ID and Password Required)*	Local Storage
Loyola Protected	**Allowed** Provided appropriate account controls are in place (MFA).	**Allowed** No special requirements, subject to any applicable laws	**Not Allowed**
Loyola Sensitive	**Allowed but Not Advised** Requires Dept. Manager approval	**Allowed** No special requirements, subject to any applicable laws	**Allowed but Not Advised** Requires Dept. Manager approval
Loyola Public	**Allowed** No special requirements	**Allowed** No special requirements	**Allowed** No special requirements

Use of central and departmental servers, where UVID authentication is required, is the best place to store all categories of Loyola data, particularly Loyola Protected data. Loyola Protected Data can be stored on the Loyola University Chicago instance of OneDrive provided access to the data is protected by Multi-Factor Authentication and sharing is set for "People in Loyola University Chicago with the link". It is never acceptable to store Loyola Protected data on any other cloud service. This includes data such as grades, social security numbers, private correspondence, classified research, etc.

Definitions:

Loyola Protected Data - Any data that contains personally identifiable information concerning any individual and is regulated by local, state, or Federal privacy regulations.

Loyola Sensitive Data - Any data that is not classified as Loyola Protected Data, but which is information that Loyola would not distribute to the general public.

Loyola Public Data - Any data that Loyola is comfortable distributing to the general public.

General Data Protection Terms:

The University must specify particular data protection terms in a contract with a cloud-computing vendor. In this way, the University creates a minimum level of security for University data. A minimum level of security ensures that the University data is kept confidential, is not changed inappropriately, and is available to the University as needed.

The University should consider the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

3.Explain the various concepts of Risk Management.

Risk Management:

Risk management is the process of identifying, assessing, and controlling threats to an organisation's system security, capital and resources. Effective risk management means attempting to control future outcomes proactively rather than reactively. Risk management allows organisations to prevent and mitigate any threats, service disruptions, attacks or compromises by quantifying the risks below the threshold of acceptable level of risks.

Process of Risk Management:

Risk management is a cyclically executed process comprised of a set of activities for overseeing and controlling risks. Risk management follows a series of **5 steps** to manage risk, it drives organisations to formulate a better strategy to tackle upcoming risks. These steps are referred to as Risk Management Process and are as follows:

- Identify the risk
- Analyze the risk
- Evaluate the risk
- Treat the risk
- Monitor or Review the risk

1. **Identify the risk** - The inception of the risk management process starts with the identification of the risks that may negatively influence an organisation's strategy or compromise cloud system security. Operational, performance, security, and privacy requirements are identified. The organisation should uncover, recognise and describe risks that might affect the working environment. Some risks in cloud computing include cloud vendor risks, operational risks, legal risks, and attacker risks.
2. **Analyze the risk** - After the identification of the risk, the scope of the risk is analyzed. The likelihood and the consequences of the risks are determined. In cloud computing, the likelihood is determined as the function of the threats to the system, the vulnerabilities, and consequences of these vulnerabilities being exploited. In analysis phase, the organisation develops an understanding of the nature of risk and its potential to affect organisation goals and objectives.
3. **Evaluate the risk** - The risks are further ranked based on the severity of the impact they create on information security and the probability of actualizing. The organisation then decides whether the risk is acceptable or it is serious enough to call for treatment.
4. **Treat the risk** - In this step, the highest-ranked risks are treated to eliminate or modified to achieve an acceptable level. Risk mitigation strategies and preventive plans are set out to minimise the probability of negative risks and enhance opportunities. The security controls are implemented in the cloud system and are assessed by proper assessment procedures to determine if security controls are effective to produce the desired outcome.
5. **Monitor or Review the risk** - Monitor the security controls in the cloud infrastructure on a regular basis including assessing control effectiveness, documenting changes to the system and the working environment. Part of the

mitigation plan includes following up on risks to continuously monitor and track new and existing risks.

The steps of risk management process should be executed concurrently, by individuals or teams in well-defined organisational roles, as part of the **System Development Life Cycle** (SDLC) process. Treating security as an addition to the system, and implementing risk management process in cloud computing independent to the SDLC is more difficult process that can incur higher cost with a lower potential to mitigate risks.

Types of Risks in Cloud Computing:

1. **Data Breach** - Data breach stands for unauthorized access to the confidential data of the organisation by a third party such as hackers. In cloud computing, the data of the organisation is stored outside the premise, that is at the endpoint of the cloud service **provider(CSP)**. Thus any attack to target data stored on the CSP servers may affect all of its customers.
2. **Cloud Vendor Security Risk** - Every organisation takes services offered by different cloud vendors. The inefficiency of these cloud vendors to provide data security and risk mitigation directly affects the organisation's business plan and growth. Also, migrating from one vendor to another is difficult due to different interfaces and services provided by these cloud vendors.
3. **Availability** - Any internet connection loss disrupts the cloud provider's services, making the services inoperative. It can happen at both the user's and the cloud service provider's end. An effective risk management plan should focus on availability of services by creating redunadancy in servers on cloud such that other servers can provide those services if one fails.
4. **Compliance** - The service provider might not follow the external audit process, exposing the end user to security risks. If a data breach at the cloud service provider's end exposes personal data, the organisation may be held accountable due to improper protection and agreements.

Apart from these risks, cloud computing possesses various security risks bound under 2 main categories.

- Internal Security Risks
- External Security Risks

Internal Security Risks:

Internal security risks in cloud computing include the challenges that arise due to mismanagement by the organisation or the cloud service provide. Some internal security risks involve:

1. **Misconfiguration of settings** - Misconfiguration of cloud security settings, either by the organisation workforce or by the cloud service provider, exposes the risk of a data breach. Most small businesses cloud security and risk management are inadequate for protecting their cloud infrastructure.
2. **Malicious Insiders** - A malicious insider is a person working in the organisation and therefore already has authorized access to the confidential data and resources of the organization. With cloud deployments, organisations lack control over the underlying infrastructure; making it very hard to detect malicious insiders.

External Security Risks:

External security risks are threats to an organisation arising from the improper handling of the resources by its users and targeted attacks by hackers. Some of the external security risks involve:

1. **Unauthorized Access** - The cloud-based deployment of the organisation's infrastructure is outside the network perimeter and directly accessible from the public internet. Therefore, it is easier for the attacker to get unauthorized access to the server with the compromised credentials.
2. **Accounts Hijacking** - The use of a weak or repetitive password allows attackers to gain control over multiple accounts using a single stolen password. Moreover, organizations using cloud infrastructure cannot often identify and respond to such threats.
3. **Insecure APIs** - The Application Programming Interfaces(APIs) provided by the cloud service provider to the user are well-documented for ease of use. A potential attacker might use this documentation to attack the data and resources of the organisation.

Need for Risk Management:

These risks need to be treated proactively by implementing risk management strategies. By implementing a risk management plan and considering the various potential risks or events before they occur, an organisation may save money and time and protect its future. In cloud computing, the organisation sets risk management plans which help them to identify appropriate cloud vendors and

service providers, make proper service-level agreements and set up better budgeting plans.

Benefits of Risk Management:

Risk management enables organisations to ensure any potential threats to cloud-deployments security, assets, and business plans are identified and treated before they derail the organisation's goals. It has far-reaching benefits that can fundamentally change the decision making process of the organisation. Here are some benefits of robust risk management:

1. **Forecast Probable Issues** - The risk management process in cloud computing identifies all the possible risks or threats associated with the cloud service provider, the cloud vendor, the organisation, and the users. It helps an organisations to mitigate risks by implementing appropiate control strategies and create a better business plan.
2. **Increases the scope of growth** - Risk management in cloud computing forces organisations to study the risk factors in detail. Thus, the workforce is aware of all the possible catastrophic events; and the organisation creates a framework that can be deployed to avoid risks that are decremental to both the organisation and the environment. Hence, risk management enables organisations to take a calculated risks and accelerate their growth.
3. **Business Process Improvement** - Risk Management requires organisations to collect information about their processes and operations. As a result, organisations can find inefficient processes or the scope for improvement in a process.
4. **Better Budgeting** - Organisations implementing risk management strategies often have clear insights into the finances. Thus, they can create more efficient budgets to implement risk management plans and achieve the organisational goals.

Data Protection Risk Cloud's Impact on IT Operations:

With IT companies switching infrastructure to cloud deployments, the risk for data protection becomes essential. The area-specific data protection laws make it hard for companies to comply with the regulations. Moreover, with personal data stored in the cloud, determining the geographical location of the data can be challenging. Therefore, it becomes difficult to hold the applicable law. Hence, developing a hurdle in the IT operations of the company.

Best Practices for Risk Management in Cloud Computing:

An effective risk management process is a mix of coordinate governance and internal controls. It coordinates the engagement of managers, employers, and stakeholders at each step to embrace risk-taking as an avenue for growth and opportunity. The following are the best practices to manage the risks in cloud computing:

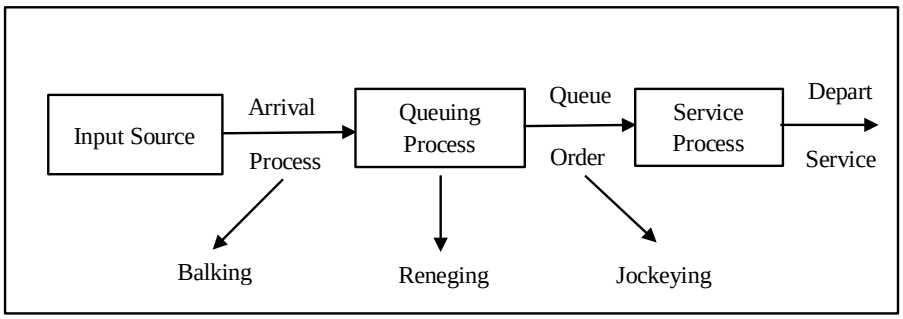
1. **Choose the cloud service provider wisely** - Perform cloud vendor risk assessment for contract clarity, availability, security, ethics, compliance, and legal liabilities. Make sure, the cloud service provider(CSP) has service providers that can deliver the services accordingly.
2. **Deploy Technical Safeguards such as Cloud Access Security Broker** - Cloud Access Security Broker (CASB) are on-premise or cloud-based software which acts as intermediary between cloud service providers and consumers, to monitor the activities and enforce organisation security policy for accessing cloud applications.
3. **Establish controls based on risk treatment** - After identification, analysis, and evaluation of the risk. Dedicated measures need to be taken to mitigate risks and drive the business processes to improve. Organisations should delete unwanted data from the hosted cloud.
4. **Optimized cloud service model** - Adopt a cloud service model that promotes achieving a business solution, minimizes risks, and optimizes cloud investment cost.
5. **Strategize Availability of Services** - Create redundancy of servers by regions and zones. In this way, if one connection fails, it will not stop the operation of the services.

4. Explain in detail about the Queuing theory in Cloud System Management.

The Queuing system in cloud service system consists of input source i.e., source of requests, queuing process which has waiting requests in the queue to be served, server process which comprises of servers to process the various requests in the queue.

Queueing theory in cloud computing:

The queuing system in cloud service system consist of input source i.e. source of requests, queuing process which has waiting requests in the queue to be served, service process which comprises of servers to process the various requests in the



queue. There can be finite capacity queuing systems or infinite capacity queuing systems and the various characteristics

Requests are generated at input source corresponding to users which seek service from the servers, the rate of arrival of request at the service system is determined by the arrival process. Various rules are followed for the selection of requests from the queue known as queue discipline or order. Service is rendered at a rate decided by the service process.

QUEUING MODELS:

This section compares and analyses the different queuing models and their study in order to enhance the clarity of usage of these models along with their specifications. Queuing models helps in estimating the performance of service systems when there is unpredictability in service times and arrival times [14].

M/M/1 MODEL:

This model is derived on the basis of certain assumptions about queuing system. It comprises of exponential distribution of inter-arrival time or Poisson‟s distribution of arrivals with mean rate „λ‟. The inter-arrival times are independently, identically and exponentially distributed in parameter λ.

M/M/C/N MODEL:

In this model, there are multiple servers in parallel to provide service to customers‟ requests. It is assumed that only one queue is formed and requests are served on a first-come, first serve basis by any of the servers. The inter-arrival times are distributed exponentially with parameter „λ‟

and the service times are distributed exponentially with an average of „μ“ customers per unit. Some example application areas of this model are: -

- Counters in library to address the service of issuing/returning books,
- Counters in telephone exchange to service the bill requests.
- Counters at the frontier to check the passports.
- Counters at tax consulting offices to receive requests concerning income and sales tax.

M/G/S MODEL:

In this model, the queuing system involves multiple servers „S“ in parallel. This model is an extension of M/M/C or M/G/1 queue where service times are exponentially distributed and a single server system respectively. The inter-arrival times in this model is exponentially distributed with parameter „λ“ and service times follow general probability distribution instead of an exponential one. It is assumed that length of inter arrival times and service periods are independent statistically This model can be deployed in systems comprising of self-service mechanisms such as restaurants with self-service filling and refilling activity, traffic light systems, etc.

5. Explain in detail about the Change Management:

Cloud Change Management:

Cloud change management facilitates changes to IT systems to minimize risks to the production environment while adhering to change management policies, audits, and risk controls.

Organizations leverage cloud change management for the following use cases:

- Data migration to the cloud
- Maintaining updated compliance requirements
- Accomplishing IT change goals

How the Cloud Impacts Change Management:

Change management is a continuous process and delivers value to an organization only if deals with agility. Cloud change management allows change leaders to anticipate and accommodate the upcoming change for better preparedness and reduced downtime.

Benefits of cloud change management:

1. Facilitates faster change implementations:

Cloud technology allows organizations to adopt an agile approach to change management. Automation and high velocity characterize cloud change management and route changes through a centralized repository for prioritization and approval.

For example, after implementing the cloud, an organization doesn't need to rely on the quarterly releases and can now continually roll out new updates.

2. Reduces time lag due to lengthy approval process:

Since changes in the cloud are self-managed, they require fewer approvals, thereby decreasing time lag. The approach shifts from change control to change enablement, thereby reducing the complexities associated with planning and execution.

3. Allows IT & business to work in sync:

A cloud management plan enables organizations to leverage infrastructure as code to plan business and IT activities effectively with mutually aligned goals.

4. Change in leadership style:

Cloud change management requires a more autonomous style of leadership by encouraging peer reviews, unlike the lengthy approval process followed by the Change Advisory Board (CAB) for traditional change management.

5. Risk Assessment:

Manual risk assessment for such a vast volume of changes isn't an accurate way to go. Change management in the cloud automates this risk assessment process for higher convenience and accuracy.

ITIL change management offers a set of best practices for delivering incident-free IT services during change projects. It helps enterprises manage risk management, establish cost-effective practices, strengthen customer relations, and create a stable IT environment that allows growth, scalability, and effective change management.

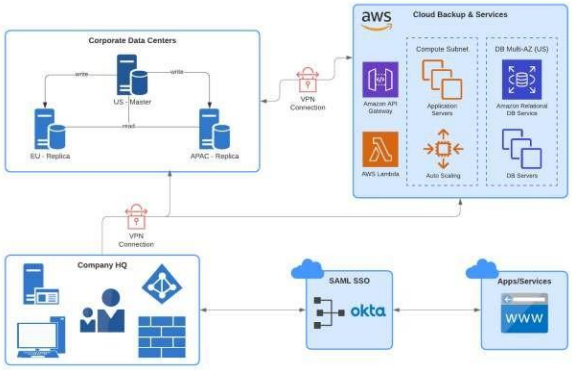
The prime objective of change agents is to align the IT goals with the organizational goals. However, cloud change management takes a holistic approach to change, and here are the key focus areas:

- **Business:** IT strategy isn't separate from the business strategy but is seen as an integral part of the business and is closely linked to all the digital transformation initiatives within the company.
- **People:** Change leaders encourage their team members to adopt cloud skills.

- **Type of Deployment:** Cloud change management process depends on the type of deployment. For a private environment, the process is simple; however, the customers' impacts are large for a shared environment, making it complicated.
- **Platform:** According to your business goals, you strategically build your principles, policies, and tools—driving your change implementation and how your company uses cloud technologies.
- **Security:** IT governance is critical to highlight non-compliance areas and develop controls for increased security.

1. Complex Processes:

Change management in the cloud is a complex process. To enable your team members to understand the architectural differences better, change practitioners must use visual aids.



2. Compliance Changes:

To keep pace with the regulatory requirements and avoid penalties, IT teams must be up to date with the compliance changes. Every industry has a different set of compliances.

For example, the healthcare industry is governed by HIPAA, which makes stringent guidelines and security protocols mandatory for certain kinds of patient health data.

3. Multi-Functional Teams Required:

Every change initiative requires cross-functional expertise. To improve flexibility and speed up the process, you can establish pre-approval for specific tasks and scenarios such as DNS updates. Change leaders can also consider using the RACI matrix for clarity in roles and responsibilities.

4. Cloud Resource Management:

Several companies shift to the cloud to increase their data storage capacity. However, if your employees use it for storing their personal information, there will

be a misuse of cloud resources. Consider establishing clear processes & policies for managing cloud usage with transparency.

The Process Flow of Cloud Change Management:

Given the complex nature of cloud deployment, here is the process flow of cloud change management to ease your transition:

1. Configuration in Cloud:

Change leaders must decide on the configuration requirements and a cloud service provider. Additionally, there must be leadership buy-in for cloud-based tools to undertake configuration changes and track the management approval process.

2. Initiate Change Management Process:

Create a robust change management plan with clear implementation timelines. Use a sandbox environment for pilot testing and then scale the initiative after making required changes.

3. Automate the Deployment:

An optimized cloud configuration will automate the deployment process, ensuring repeatability and consistency across multiple environments and enabling automation of testing procedures. Automation does not guarantee a successful change implementation; it reduces risk and brings standardization.

For example, if an automated security test is pre-approved for deployment purposes, there is no security review requirement during the change approval process.

4. Use Change Management Tools to Drive Change:

With every change initiative, employee upskilling and reskilling becomes a challenging task. Implementing digital adoption platforms(DAP) alongside your cloud implementation will take you a step closer to effortless change roll-outs.

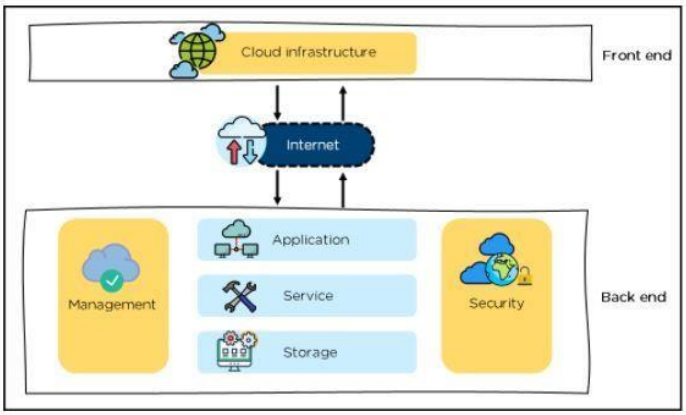
5. Review & Record the Process:

Since cloud change management is a continuous process, organizations need to schedule regular feedback mechanisms, make required iterations and document the process for future reference.

7. Describe the concepts of Cloud service architecture.

Cloud Computing Architecture:

Cloud Computing Architecture is divided into two parts, i.e., front-end and back-end. Front-end and back-end communicate via a network or internet. A diagrammatic representation of cloud computing architecture is shown below:



Cloud Computing Architecture:

Front-End:

- It provides applications and the interfaces that are required for the cloud-based service.
- It consists of client's side applications, which are web browsers such as Google Chrome and Internet Explorer.
- Cloud infrastructure is the only component of the front-end. Let's understand it in detail.

Front-end - Cloud Computing Architecture:

- Cloud infrastructure consists of hardware and software components such as data storage, server, virtualization software, etc.
- It also provides a Graphical User Interface to the end-users to perform respective tasks.

Back-End:

It is responsible for monitoring all the programs that run the application on the front-end

It has a large number of data storage systems and servers. The back-end is an important and huge part of the whole cloud computing architecture, as shown below:

Back-end - Cloud Computing Architecture:

The components of the back-end cloud architecture are mentioned below. Let's understand them in detail one by one.

Application:

- It can either be a software or a platform

- Depending upon the client requirement, the application provides the result to the end-user (with resources) in the back end

Service:

- Service is an essential component in cloud architecture
- Its responsibility is to provide utility in the architecture
- In a Cloud, few widely used services among the end-users are storage application development environments and web services

Storage:

- It stores and maintains data like files, videos, documents, etc. over the internet
- Some of the popular examples of storage services are below:
- Amazon S3
- Oracle Cloud-Storage
- Microsoft Azure Storage
- Its capacity varies depending upon the service providers available in the market

Management:

- Its task is to allot specific resources to a specific task, it simultaneously performs various functions of the cloud environment
- It helps in the management of components like application, task, service, security, data storage, and cloud infrastructure
- In simple terms, it establishes coordination among the cloud resources

Security:

- Security is an integral part of back-end cloud infrastructure
- It provides secure cloud resources, systems, files, and infrastructure to end-users
- Also, it implements security management to the cloud server with virtual firewalls which results in preventing data loss

Benefits of Cloud Computing Architecture:

The cloud computing architecture is designed in such a way that:

- It solves latency issues and improves data processing requirements
- It reduces IT operating costs and gives good accessibility to access data and digital tools
- It helps businesses to easily scale up and scale down their cloud resources
- It has a flexibility feature which gives businesses a competitive advantage

- It results in better disaster recovery and provides high security
- It automatically updates its services
- It encourages remote working and promotes team collaboration

UNIT-III CLOUD SERVICES MANAGEMENT

Cloud service reference model, **Cloud service life cycle**, Basics of cloud service design, dealing with legacy systems and services, **Benchmarking of cloud services**, Cloud service capacity planning, Cloud service Deployment and migration, Cloud marketplace, Cloud service operations management

PART-A

1. Define Reference Model.
2. List out the function layers of cloud computing reference model.
3. What are the different stages of cloud computing life cycle?
4. Why we need a service catalog?
5. What is Benchmarking in the Cloud?
6. Define Cloud Migration:
7. What are the benefits of cloud migration?
8. Llist out the cloud migration deployment methods
9. Why we need cloud capacity planning?
10. What are the key components of cloud capacity planning?
11. Is cloud marketplace suitable for all types of clouds? Justify.
12. List out the advantages of cloud services design.
13. What is the right choice for dealing with legacy systems?
14. Does the service design catalogue contain networking options?
15. Name the steps in capacity planning.
16. Sketch the view of cloud services design.
17. Name the steps in capacity planning.
18. Is the cloud migration deployment model suitable for all types of deployment models? Justify.
19. Give the importance of cloud capacity management.
20. State the process flow in change management.

21. What is meant by capacity utilization and utilization rate formula?
22. List out the goals of capacity planners.
23. Define baseline measurement and load metrices.
24. List the benefits of cloud migration.

PART-B:

1. Explain in detail about the cloud computing reference model.
2. Explain in detail about the Cloud Service Life Cycle:
3. Explain in detail about the Benchmarking in cloud computing.
4. Explain in detail about the Cloud migration deployment.
5. Descibe the concepts of cloud capacity planning

PART-A

1. Define Reference Model.

The Cloud Computing Reference Model is an abstract model that defines the cloud vocabulary and design elements, the set of configuration rules, and the semantic interpretation.

3. List out the function layers of cloud computing reference model.

The Cloud Computing Reference Model is divided into three cross functional Layers:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

3. What are the different stages of cloud computing life cycle?

- ✓ Service strategy
- ✓ Service design
- ✓ Service transition
- ✓ Service operation
- ✓ Service improvement
- ✓ Service retirement

4. Why we need a service catalog?

A service catalog is helpful to identify your cloud users to determine their needs. The role of the service catalog is to bridge that gap. The service catalog enables IT to define the areas of configuration and choice that users can select, according to their role.

5. What is Benchmarking in the Cloud?

Benchmarking in the cloud is a practice that measures and documents the current performance and configurations of an application environment. Cloud baselines support application discovery in the sense that both are used in the Validation stage or the post-migration stage where the cloud migration assessment is performed.

6. Define Cloud Migration:

Cloud migration is a general term used to designate transferring digital operations from one site to a cloud platform. When you migrate to the cloud, it encompasses data, processes, and applications to third-party servers.

7. What are the benefits of cloud migration?

- Scalability
- Cost
- Security
- Flexibility
- Disaster Recovery

8. Llist out the cloud migration deployment methods

- Hybrid Deployment
- Multicloud Deployment
- Understanding the Cloud Migration Process

9. Why we need cloud capacity planning?

Cloud capacity planning aims to match demand with available resources. It analyzes what systems are already in place, measuring their performance and predicting demand. Your organization can then provision and allocate cloud resources based on that demand.

10. What are the key components of cloud capacity planning?

- ✓ Demand forecasting
- ✓ Performance analysis
- ✓ Cost management.
- ✓ Contingency planning
- ✓ Integration considerations
- ✓ Feedback loops

11. Is cloud marketplace suitable for all types of clouds? Justify.

Yes, All purchases are made through a single cloud vendor, rather than routing thousands of products through different vendors for approval. Cloud marketplaces also **provide a single source of billing and invoicing**,

12. List out the advantages of cloud services design.

- Accessibility anywhere, with any device.
- Ability to get rid of most or all hardware and software.
- Centralized data security.
- Higher performance and availability.
- Quick application deployment.
- Instant business insights.
- Business continuity.

13. What is the right choice for dealing with legacy systems?

One alternative to completely replacing or maintaining legacy systems is to **modernize them**. Modernized systems might be more cost-effective, while increasing efficiency and improving existing processes at the same time

Price-performance and cost savings.

14. Does the service design catalogue contain networking options?

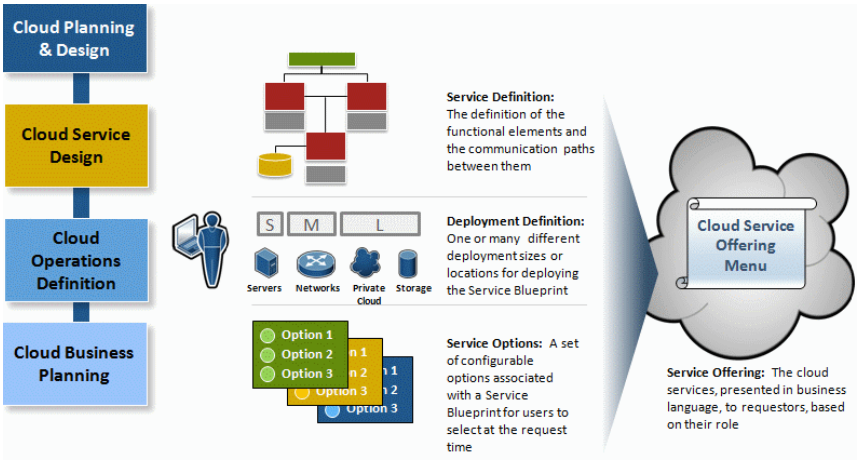
Yes,It supports all networking connections and deals with all services.

A service catalog (or catalogue), is **an organized and curated collection of business and information technology services within an enterprise**. Service catalogs are knowledge management tools which designate subject matter experts (SMEs) who answer questions and requests related to the listed service

15. Name the steps in capacity planning.

1. Forecast your anticipated demand.
2. Determine required capacity.
3. Calculate the resource capacity of your current team.
4. Measure the capacity gap.
5. Align capacity with demand

16. Sketch the view of cloud services design.



17. **Name the steps in capacity planning.**

- Forecast your anticipated demand.
- Determine required capacity.
- Calculate the resource capacity of your current team.
- Measure the capacity gap.
- Align capacity with demand.

18. **Is the cloud migration deployment model suitable for all types of deployment models? Justify.**

Each deployment model is defined according to where the infrastructure for the environment is located. There are three main cloud service models: Software as a Service, Platform as a Service, and Infrastructure as a Service.Yes it is suitable for all types.

19. **Give the importance of cloud capacity management.**

Capacity management **makes it possible to predict the future behavior of system resources in scenarios such as these and many others, as well as the resulting impact on business KPIs**. This helps IT correlate business needs to capacity demand and align resources as needed to support them.

20. **State the process flow in change management.**

1. Prepare the Organization for Change. ...
2. Craft a Vision and Plan for Change. ...
3. Implement the Changes. ...
4. Embed Changes Within Company Culture and Practices. ...
5. Review Progress and Analyze Results.

21. **What is meant by capacity utilization and utilization rate formula?**

What is the formula for Utilisation rate?

Calculating the utilization rate consists of **dividing an employee's total billable hours by the total available hours**. In order to express the rate in percentage form, the resulting figure should be multiplied by 100.

22. **List out the goals of capacity planners.**

The main objective of capacity planning is to ensure optimal resource allocation in an organization, aligning the right amount of resources with the specific timing to effectively meet customer demands. The key objectives include: **Meeting customer expectations by providing products or services promptly**

23. **Define baseline measurement and load metrices**.

The metrics baseline consists of **data collected in previous projects**. They can be used to set a goal and try to determine if trends show the likelihood of meeting that goal. They become an essential piece of a key performance indicator (KPI).

24. **List the benefits of cloud migration.**

- Optimised costs. ...
- Flexibility and scalability. ...
- Enhanced security. ...
- Compliance. ...
- Backup, recovery and failover. ...

PART-B:

1. Explain in detail about the cloud computing reference model.

The Cloud Computing Reference Model is an abstract model that defines the cloud vocabulary and design elements, the set of configuration rules, and the semantic interpretation.

The Cloud Computing Reference Model is divided into three cross functional Layers:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

Software as a Service (SaaS):

Software as a service is a software delivery model where licensed software, usually on a subscription basis, is centrally hosted and used by customers over the internet via a web browser or through client software. It is also referred to as on-demand software or web-based/web-hosted software.

SaaS is currently the most common cloud computing service. Day-to-day workforce applications such as Slack, Zoom, and Customer Resource Management (CRM) software are prime examples of SaaS.

Platform as a Service (PaaS)

Platform as a Service is a cloud computing model which provides customers with a complete platform to develop and run their applications. This includes hardware, software, infrastructure like servers, storage, databases, and development tools hosted at the vendor's data centre. This helps avoid the cost, complexity, and inflexibility of maintaining this on-premise. Developers can build and deploy apps on the cloud without worrying about the underlying architecture and resource constraints. The cloud provides them with the ability to scale up on demand and also scale down during idle & low-traffic periods.

Infrastructure as a Service (IaaS)

Infrastructure as a Service is a cloud computing model that deals with fundamental computing, network and storage. Contrary to PaaS, it provides the lowest level of resources on the cloud.

Cloud Reference Model:

The NIST cloud computing model comprises five crucial features:

- Measured Service

- On-demand self-service
- Resource pooling
- Rapid elasticity
- Broad network access

They follow the same three service models defined earlier: SaaS, PaaS and IaaS, and mention four deployment models: i.e., Private, Community, Public, and **Hybrid cloud.**

The CSA Cloud Reference Model:

Security in the cloud is a rising concern. With so much data being available and distributed on the cloud, vendors must establish proper controls and boundaries. The **Cloud Security Alliance (CSA)** reference model defines these responsibilities. It states that IaaS is the most basic level of service, followed by PaaS and then SaaS. Each of them inherits the security intricacies of the predecessor, which also means that any concerns are propagated forward. The proposal from the CSA is that any cloud computing model should include the below-mentioned security mechanisms:

- Access control
- Audit trail
- Certification
- Authority

The OCCI Cloud Reference Model:

The Open Cloud Computing Interface (OCCI) is a set of specifications and standards that defines how various cloud vendors deliver services to their customers. It helps streamline the creation of system calls and APIs for every provider. This model not only helps with security but also helps create managed services, monitoring, and other system management tasks that can be beneficial. The main pillars of the OCCI cloud computing reference model are:

- **Interoperability** – Enable diverse cloud providers to operate simultaneously without data translation between multiple API calls
- **Portability** – Move away from vendor lock-in and allow customers to move among providers depending on their business objectives with limited technical expenses, thus fostering competition in the market
- **Integration** – The feature can be offered to the customer with any infrastructure

- **Extensibility** – Using the meta-model and discovering features, OCCI servers can interact with other OCCI servers using extensions.

2. Explain in detail about the Cloud Service Life Cycle:

The cloud service lifecycle is the process that cloud providers use to design, develop, deploy, and manage cloud services. It involves a set of stages that a cloud service goes through, from ideation and planning to retirement. The cloud service lifecycle typically consists of the following stages.

1. Service strategy: This is the initial stage where the provider identifies and evaluates potential cloud services. They consider factors like market demand, competition, and organizational goals.

2. Service design: In this stage, the provider determines the technical and functional requirements of the service, and the resources needed to develop and implement it. They also design the architecture and infrastructure of the service.

3. Service transition: This stage involves the deployment of the service to the cloud environment. The provider tests the service and ensures that it meets the required standards, security protocols, and quality expectations.

4. Service operation: This is the stage where the provider delivers the service to the users, monitors it for performance, and maintains it as required. They also provide customer support and manage service disruptions and other incidents.

5. Service improvement: In this stage, the provider continuously reviews and evaluates the service for optimization and improvement. They use feedback from users to identify areas for improvement and make necessary changes to enhance the service's performance, reliability, and availability.

6. Service retirement: This is the final stage in the lifecycle, where the provider decides to retire the service when it is no longer needed or viable. They ensure that user data is safely transferred or deleted, and take any other necessary measures to close the service down.

The cloud service lifecycle helps providers to manage their services effectively and ensure that they meet customer needs and organizational goals.

The Cloud Service Lifecycle is the process of delivering and managing cloud services over their entire lifecycle. It consists of four phases: Service Strategy, Service Design, Service Operation, and Service Retirement.

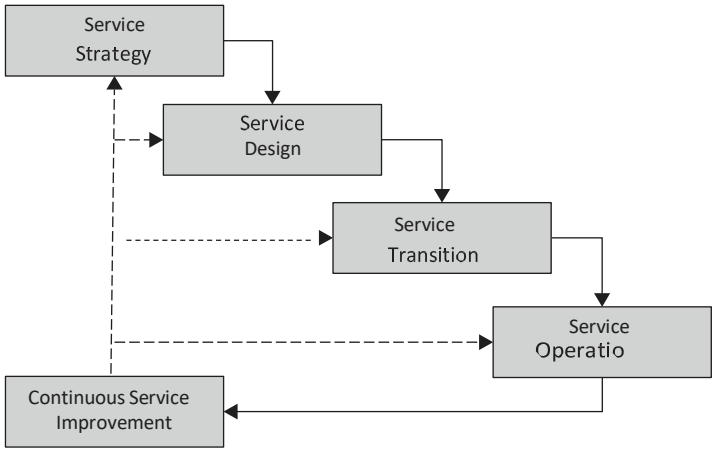
1. Service Strategy: In this phase, the business goals and objectives of the cloud

service are identified, and a plan is created to meet those goals and objectives. The service provider should determine the target market, the pricing model, the service level agreement (SLA), and the key performance indicators (KPIs) for the service.

2. Service Design: In this phase, the service provider designs the cloud service to meet the identified business goals and objectives. This includes determining the technical requirements, the architecture of the service, and the processes for managing the service. In this phase, the service provider must consider the security, privacy, and compliance requirements of the service.

3. Service Operation: In this phase, the cloud service is made available to the customers. The service provider must monitor the service to ensure it is performing as expected and meet the SLA and KPIs. The service provider must also provide customer support and resolve any issues that arise.

4. Service Retirement: In this phase, the service provider determines when to retire the cloud service. This may be due to changes in business requirements, or the



service may have reached its end of life. The service provider must ensure that customers are given adequate notice and have a plan to migrate to a new service. The service provider should also ensure that data is properly disposed of according to the security and privacy policies.

3. Explain in detail about the Benchmarking in cloud computing.

Benchmarking in the cloud is a practice that measures and documents the current performance and configurations of an application environment.

Cloud baselines support application discovery in the sense that both are used in the Validation stage or the post-migration stage where the cloud migration assessment is performed. Without application discovery, it would be a challenge to generate cloud baselines because you don't know what resources you are getting

baselines from. Without cloud baselines, knowing how your current environment is structured would not make sense at all because you're going to move them to the cloud anyway

For user experience metrics, you should review the business objectives you have defined at the onset of your planning. Then generate baselines around those objectives. For instance, one of your business objectives is to improve the time it takes to process a transaction. You can then measure the peak and average process times for n transactions in a time range where there are a.) more users than usual and b.) fewer users than usual.

Benchmarking Challenges

The benchmarking is important in cloud migrations. It is also beneficial for you to take into account the possible challenges that you may encounter when generating performance and configuration baselines.

1. Long Preparation & Execution Time for Manual Benchmarking

Gathering data when generating baselines may take some time to execute if you don't have a tool capable of exporting performance and configuration reports. Performing benchmarking manually means having to log in to the device(s) directly, capturing data points from manual queries or GUI-based wizards, refining them to support your defined business objectives and established KPIs, and organizing them in accordance with how your environment is structured.

2. Dynamic Nature of Distributed Systems

Distributed systems in production are always changing. The baselines generated at any given time may no longer represent the target behavior of your systems after migration. This is why it is important that aside from the validation stage, which is often only performed once, your target systems in the cloud should readily be available for monitoring. This allows you to capture data right after the migration activity for hyper-care monitoring purposes.

3. Performance Isolation

In distributed systems, the behavior of an application may be influenced by other applications and services running simultaneously. This makes it difficult to measure the performance metrics of each component separately without a tool capable of discovering them as individual components. It may result in service degradation and performance interference.

Generating Cloud Baselines in IT-Conductor

The common performance baselines you need to capture are the resource utilization metrics such as CPU/Memory, storage, and network. In IT-Conductor, you can capture those metrics from the service grid. You can easily drill up/down components in the service grid to capture the different metrics you need in generating performance baselines for your source environment.

4. Explain in detail about the Cloud migration deployment.

Cloud Migration:

Cloud migration is a general term used to designate transferring digital operations from one site to a cloud platform. When you migrate to the cloud, it encompasses data, processes, and applications to third-party servers.

Benefits of Cloud Migration:

There are several advantages when a company decides to migrate to the cloud. By choosing a cloud-based solution, organizations can deliver enhanced performance while staying on top of technology's latest innovation.

The four primary benefits that companies derive from cloud migration include:

Scalability:

Migration to cloud platforms allows a company to efficiently scale its IT requirements up or down based on its current demands. It can be difficult to service customers' changing demands if operations are locked to a legacy (outdated, but still in use) infrastructure.

Switching to the cloud allows businesses to drastically alter their operations and infrastructure to facilitate the current demands without being restricted to quickly depreciating equipment. The power to promptly scale a company's workload allows it to tailor its resource allocation effectively.

Cost:

Organizations that opt for cloud services can substantially reduce operational costs and unnecessary overhead. They will no longer be tied to leasing equipment or expensive physical locations, meaning these resources can be put to better use, such as product development.

Security:

If maintained correctly in the shared security responsibility model, migrating to the cloud can reduce security flaws found on traditional network systems.

Flexibility:

Through cloud migration, users can be authorized to access the necessary services, regardless of their geographical location and their preferred device. This flexibility creates previously impossible opportunities, allowing a company to branch into new territories, source talent globally, and expand alongside business demand.

Disaster Recovery:

The duty of disaster recovery is also simplified thanks to many service providers offering backup and logging functionality. With these protocols integrated into standard practices, issues can be quickly identified and remedied without a team needing to be on-site.

By implementing sound and well-thought-out cloud migration strategies, companies can easily take advantage of reduced costs, scalable solutions, a secure environment, flexible operations, and greater access to enhanced functionality.

Cloud Migration Strategies:

There are four primary migration strategy approaches that companies can use when improving their operations.

Rehost:

Rehosting (also known as Lift and Shift) essentially takes an existing system and transfers it to a cloud-based platform. By choosing an IaaS (Infrastructure as a Service) provider, the organization recreates its application architecture on top of new infrastructure.

This approach requires minimal intervention and refactoring, which makes it a quick procedure. However, by opting to rehost, the company forgoes many benefits derived from a cloud provider's native applications.

Companies with low demands from their cloud operations or currently run on several virtual machines can experience the greatest benefit from this route.

Rehosting may be the quickest method of cloud migration, with some providers even offering automated tools, but it comes at the cost of optimization.

Refactor:

Refactoring shares similarities to rehosting. A business will reuse its existing code and framework but will place it on a PaaS (Platform as a Service) instead of an IaaS.

Revise:

Revising is a migration strategy that uses part of an existing codebase while rewriting or expanding on it before moving it to either an IaaS or PaaS.

A company can maintain many of its applications, but with the added benefit of cloud-native services, such as scaling or automation.

Replace:

The final migration strategy is the most drastic. Replacing is for a company to scrap its entire current system and move over to a SaaS (Software as a Service) platform. Replacing a system can be an enticing option for those who haven't updated their operations for some time or have invested little into their current systems.

Cloud Migration Deployment Methods:

Understanding the different cloud migration strategies is one part of the solution. The other is deployment.

Hybrid Deployment:

A hybrid deployment sees a mixed combination of data centers across multiple environments. Using this method, a company can have data centers on public clouds, private clouds, or on-site locations.

While this method allows an organization to take advantage of cloud functionality, it also requires more cohesive communication between the environments.

Multicloud Deployment:

Multicloud deployment sees operations spread across multiple public cloud platforms. This method allows a company to mix and match applications from different cloud providers while also offering redundancy and backup features.

Single Cloud Deployment:

Smaller businesses that only require a single cloud provider's product line may opt for single cloud deployment. While this may be the easiest deployment method for cloud migration, it's also the most limiting.

Understanding the Cloud Migration Process:

Several aspects need to be considered to know which migration strategy and deployment method are best for a company.

Goals and Budget:

Only by knowing what a company wants can it measure to assess its success.While this may be a challenging aspect to come to terms with, the costs associated with migrations need to be offset by the Return on Investment (ROI).

Migration Strategy:

The migration strategy should act as a roadmap listing various milestones and objectives to keep the plan on track. The plan must incorporate:

- Realistic timelines
- Accounting for variables and dependencies
- Current cloud operational maturity
- Validation of benefits to business application
-

5. Descibe the concepts of cloud capacity planning.

Cloud capacity planning aims to match demand with available resources. It analyzes what systems are already in place, measuring their performance and predicting demand. Your organization can then provision and allocate cloud resources based on that demand.

Best Practices of Cloud Capacity Planning:

Below are some best practices to leverage cloud capacity planning for your organization:

Evaluate:

To achieve optimal performance cost-effectively, you must first evaluate your workload capacity requirements. Evaluating your current workloads before moving them to the cloud is essential. It is important to think about why workloads change and what happens when they do.

Review:

Next, look at your metrics to see how you use your infrastructure and how much capacity it needs. Your review should include instances when your usage spikes, as well as an assessment of how often these spikes occur, how big they are, and how long they last. Via utilization patterns, you can identify spikes and dips in server, application, and system usage. You'll need to consider business forecasts and historical trends. For example, knowing the capacity demands of a new customer for the following quarter can help you prepare a stronger plan.

Strategize:

To develop a cloud capacity planning strategy, you should assess your past infrastructure and capacity through feedback from business stakeholders. Whenever possible, automate the provisioning and deployment of cloud resources as part of your strategy. Your strategy should include a disaster recovery plan that details recovery times for your applications, systems, and servers. It should also discuss the potential impact and cost of downtime due to disaster.

Ensure:

Make sure your quotas match your capacity needs. A quota is a specific countable resource, like how many load balancers your projects can use simultaneously. Your goal in your cloud capacity planning effort should be to support business goals. You should be able to tell users what will happen with the cloud in three to six months regarding cost, response time, and availability

Benefits of Cloud Capacity Planning:

A number of benefits from cloud capacity planning, including:

Reduction of Costs:

A strategic cloud capacity plan helps IT anticipate and plan for changes that may affect cloud resource management. Your IT team can better control, track, and adjust resource capacity, consumption, and related budgets or quotas when they understand business priorities and plans.

Application Performance

Poor performance can lead to negative user experiences and increased customer churn. As part of strategic cloud capacity planning, IT can find and fix performance bottlenecks from systems and applications. Additionally, cloud capacity planning helps you find cost-effective ways to achieve optimal performance.

Agility

Your IT team can effectively plan for unforeseen spikes in demand using historical data and usage patterns as part of effective cloud capacity planning.

Cloud Capacity Planning and Synopsys:

Cloud capacity planning can aid any organization that uses cloud computing to improve performance. Chip makers and small businesses looking to leverage the cloud for their chip projects can benefit immensely from cloud capacity planning.

Synopsys, EDA, and the Cloud:

Synopsys is the industry's largest provider of electronic design automation (EDA) technology used in the design and verification of semiconductor devices, or chips. With Synopsys Cloud, we're taking EDA to new heights, combining the availability of advanced compute and storage infrastructure with unlimited access to EDA software licenses on-demand so you can focus on what you do best – designing chips, faster. Delivering cloud-native EDA tools and pre-optimized hardware platforms, an extremely flexible business model, and a modern customer experience, Synopsys has reimagined the future of chip design on the cloud, without disrupting proven workflows.

Dynamic needs: Startups can experience rapid growth, making it essential to be prepared for sudden increases in user bases and data volumes to avoid system outages or performance issues.
Cost efficiency: With often limited budgets, your startup needs to avoid over-provisioning and under-provisioning, which can lead to missed opportunities.
Optimal performance: Capacity planning helps manage loads for consistent performance even during traffic spikes.
Investor confidence: Showing a clear understanding of cloud infrastructure needs and scalability attracts and retains investors, highlighting operational maturity.
Future-proofing: Capacity planning prepares startups for technological shifts, promising long-term agility and competitiveness.
"Capacity management is the most underestimated problem of cloud computing," says Morgan Stanley, executive director for IT strategy at Evangelos Kotsovinos. "One of the main reasons for using cloud computing services is to get efficiency and cost savings. And maximum IT efficiency on the cloud comes from good capacity planning and management."

Key components of cloud capacity planning:

Cloud capacity planning isn't a one-and-done task on your to-do list, nor is it a singular activity. It's a combination of interrelated components, each of which is critical in aligning your cloud resources with your business needs.
Here's a breakdown of the must-have elements of effective cloud capacity planning:
Demand forecasting: Analyze historical data and current trends to anticipate future cloud resource needs.
Performance analysis: Use tools (like DigitalOcean Monitoring) to track resource performance, guiding decisions on scaling needs.
Cost management: Understand both direct and indirect costs of cloud resources to optimize spending without compromising performance.
Contingency planning: Prepare for unexpected events (from traffic spikes to system failures) by having backup resources or strategies in place.
Integration considerations: Create seamless integrations of multiple cloud services or transitions between on-premises and cloud solutions without resource conflicts.
Feedback loops: Continuously revisit and adjust capacity plans based on real-world performance and evolving business needs.

Cloud capacity planning best practices and strategies

Cloud capacity planning for your startup can sometimes feel like steering a sailboat onto shore without a lighthouse. There can be lots of uncertainty and guesswork that undermine your confidence.

1. Regularly review and adjust plans:

Cloud environments are dynamic, and your capacity plans need to be, too. Regularly reviewing your current usage against your forecasts will help you identify trends and make necessary adjustments.

2. Embrace automation and auto-scaling:

Modern cloud platforms offer auto-scaling features that automatically adjust resources based on demand. This prevents your performance from dropping when there's a spike in traffic or user demands.

For example, DigitalOcean's autoscaling dynamically adjusts your computing resources based on the current workload. This helps you meet demands without overpaying for what you don't need.

3. Invest in monitoring and analytics tools:

Without data and analysis, you're just guessing at your startup's cloud demands. Real-time monitoring provides insights into resource utilization, helping in proactive adjustments—AKA making changes *before* something goes wrong.

Use DigitalOcean Monitoring and third-party analytics tools to get a comprehensive view of your resource usage and performance metrics. This gives you a better understanding of your capacity requirements.

4. Train and upskill your team:

A well-informed team can make better capacity planning decisions and quickly address issues. Invest in training sessions, workshops, or online courses to keep your team up-to-date with the latest cloud capacity management techniques.

5. Test different scenarios:

Simulating different usage scenarios can help you understand how your cloud infrastructure responds to various loads. Periodically run stress tests or load testing to simulate high-demand scenarios and see how your cloud resources cope.

6. Study workload patterns:

Different applications and services have varying usage patterns. Some might experience steady traffic, while others have peak periods. Understanding these patterns helps in making informed capacity management decisions.

For example, if performance drops on the weekends or holidays, you know you might be experiencing increased traffic to your websites or applications.

Analyze historical data to identify patterns. Use this information to allocate resources to handle peak loads without overcommitting during off-peak times.

7. Plan for data transfer costs:

While most focus is on cloud computing and storage costs, data transfer costs can also be significant. If you're moving large volumes of data in and out of the cloud, this is a metric you'll want to keep an eye on.

Monitor data transfer volumes and costs. Consider strategies like data compression or caching to reduce transfer costs.

8. Collaborate across departments:

Capacity planning shouldn't be an isolated IT function. Collaborate with other departments, such as sales and marketing, to understand upcoming campaigns or product launches that might impact cloud resource needs.

Hold cross-departmental meetings to discuss upcoming initiatives and their potential impact on cloud resources.

9. Document your plan:

Having a well-documented capacity plan makes it easier to onboard new team members and serves as a reference for future planning. Maintain a centralized documentation repository, detailing your capacity management, decisions made, and lessons learned for future reference.

UNIT-IV CLOUD SERVICE ECONOMICS

Pricing models for cloud system-Freemium-Pay per reservation-subscription based charging-procurement of cloud services-capes vs opex shift-cloud service-charging-cloud cost models.

PART-A

1. What are the types of pricing models in cloud computing?
2. Define Freemium.
3. What is meant by cost management?
4. What are the importance of cloud cost management?
5. Differentiate between Cloud Cost Management vs. Cloud Cost Optimization
6. Define CapEx :
7. List out the characteristics of CapEx expenditure:
8. What is OpEx in Cloud?
9. Write a short note on pay-per-use on model.

PART-B:

1. Explain in detail about the pricing models for cloud services.
2. Describe the concepts of Freemium.
3. Explain in detail about the cloud cost management.
4. Describe the cloud cost models.
5. Explain in detail about the Opex and capex.

PART-A

1. What are the types of pricing models in cloud computing?

- Fixed Pricing Models
- Pay-per-use Model
- Pay-per-use Model

2. **Define Freemium**.

Freemium is a business model that works by offering a product or service free of charge (like software, web services etc) while charging a premium for advanced features and functionality.

3. What is meant by cost management?

Cloud cost management is an organizational practice that helps businesses understand and manage the costs and requirements associated with cloud technologies. Its main goal is to find more efficient cost-effective ways to use the cloud.

4. What are the importance of cloud cost management?

Cloud computing offers major advantages, including rapid scalability and the elimination of upfront capital investments. Cloud solutions allow DevOps and IT teams to start using services quickly and easily, but they also introduce a risk of unexpected costs that exceed your planned budget. You can implement a cloud cost management approach to help plan your organization's future cloud service consumption and costs.

5. Differentiate between Cloud Cost Management vs. Cloud Cost Optimization

Cloud cost management involves allocating and tracking cloud resources to analyze and report cloud spending. Cloud cost optimization takes these insights to help you understand how to minimize costs while maximizing business value.

Cloud cost optimization is not limited to cost savings—aligning costs with business goals is also important. When revenue increases, increasing costs might not be an issue.

Cloud cost growth often relates to indicators such as introducing new customers and launching new features. However, these activities usually bring higher returns. In software-as-a-service (SaaS) environments, higher revenues often lead to higher profit margins and help attract investors.

6. Define CapEx :

CapEx is short for capital expenditure. **Capital expenditure is the cost a business incurs to acquire assets that will provide benefits beyond the current year.** CapEx is also referred to as PP&E, which stands for Property, Plant, and Equipment.

7. List out the characteristics of CapEx expenditure:

- Long-term
- Approval
- Ownership
- Upfront cost
- High-ticket
- On-premises
- Tax treatment

8. **What is OpEx in Cloud?**

Operational expenses in the cloud are costs associated with public, private, hybrid, and/or multitenant environments. Unlike cloud CapEx, OpEx assets and services are rented by the user using a subscription model and are solely owned by the provider.

9. Write a short note on pay-per-use on model.

In this model, user only have to pay for what they use. Customer pays in function of the time or quantity he consumes on a specific service. Amazon Web Services (AWS) [13], Salesforce [19]

PART-B:

1. Explain in detail about the pricing models for cloud services.

Pricing on the cloud:

Many things are taken into consideration when talking about pricing on the cloud, first thing is that the service provider's aims to maximize the profit and the customers are looking for a higher quality of services with a lower price.

Second, selling services on the cloud is very competitive due to the high number of providers that are selling the same services. In addition, prices are influenced by:

- The lease period, which can be considered as the contract time between the provider and the customer.
- The initial cost of the resources
- The rate of depreciation, which means how many time these resources are being used
- The quality of service
- The age of the resources
- The cost of Maintenance

Pricing Models

There are many pricing models used on cloud, and they can be classified in two main types from the perspective of the changing period: fixed and dynamic.

Fixed Pricing Models

Fixed pricing models are also called Static pricing models, due to the stability of the price for a long time. The most famous service providers on the cloud such as Google, Amazon Web Services, Oracle, Azure and others use fixed pricing models.

Fixed Pricing makes users aware of the cost of doing business and consuming a resource. However, in the other hand this type of pricing is mostly unfair with the customers because they can overpay or underpay for their needs. In addition, it is not affected with the demand.

There are many fixed pricing such as "pay-per-use", subscription, price list … In this part I will talk briefly about these pricing models:

Pay-per-use Model

In this model, user only have to pay for what they use. Customer pays in function of the time or quantity he consumes on a specific service. Amazon Web Services (AWS) [13], Salesforce [19] as shown in Table 1 and Table 2 use this model.

	Standard Storage	Reduced Redundancy storage
First 1 TB / month	0.0390$ / GB	0.0312$ / GB
Next 49 TB / month	0.0383$ / GB	0.0306$ / GB
Next 450 TB / month	0.0377$ / GB	0.0301$ / GB
Next 500 TB / month	0.0370$ / GB	0.0296$ / GB
Next 4000 TB / month	0.0364$ / GB	0.0291$ / GB
Over 5000 TB / month	0.0357$ / GB	0.0285$ / GB

Table 1 — Amazon S3 storage pricing

Product	Description	Price (per user per month)
Contact Manager	Contact management for up to 5 users	5$
Group	Basic sales & marketing for up to 5 users	25$
Professional	Complete CRM for any size team	65$
Enterprise	Customize CRM for entire business	125$
Unlimited	Unlimited CRM power and support	250$

Table 2 — Salesforce Cloud pricing

Subscription

In this model, users pay on a recurring basis to access software as an online service to profit from a service. The customer subscribe to use a preselected combination of service units for a fixed and a longer frame, usually monthly and yearly.

Dropbox [16] — like shown in Table 3 — uses this model.

	Basic (Free)	Plus (8.25$/month)	Professional (16.58$/month)
Storage	2 GB	1 TB	1 TB
Anywhere access	✓	✓	✓
Smart Sync	×	×	✓
Full text search	×	×	✓
Mobile offline folders	×	✓	✓
Camera Upload	✓ (with desktop client installed)	✓	✓
Document scanning	✓	✓	✓

Table 3 — Dropbox pricing

Hybrid

This model is a combination of the pay-per-use and subscription pricing models, in this model all services prices are set using the subscription model but when the use limitation exceed, pay-per-use pricing is used.

This model is used by Google app engine [12] like shown in Table 4.

Resource	Free quota per day	Unit	Price beyond the free quota per unit
Stored data	1 GB	Per GB per month	0.18 $
Entity reads	50000	Per 100K entities	0.06 $
Entity writes	20000	Per 100K entities	0.18 $
Entity deletes	20000	Per 100K entities	0.02 $

Table 4 — Google app engine pricing

Pay for resources

In this model, a customer pays for resources utilized. This model is used by Microsoft Azure in the Infrastructure as a service pricing as shown in Table 5 [14].

Instance	Cores	RAM	Temporary storage	Price
A0	1	0.75 GB	20 GB	0.02$ /hour
A1	1	1.75 GB	225 GB	0.08$ /hour
A2	2	3.50 GB	490 GB	0.16$ /hour
A3	4	7.00 GB	1000 GB	0.32$ /hour
A4	8	14.00 GB	2040 GB	0.64$ /hour

Table 5 — Windows Azure IaaS pricing

Price List

In this model, the service provider lists all prices and their details in one table/list. In addition, it can be downloaded as a document (PDF). This model is used by Oracle [15] as shown in Fig. 1.

Oracle Application Specific Technology Products

	Named User Plus	Software Update License & Support	Processor License	Software Update License & Support	Employee for HCM	Software Update License & Support
Application Server Products						
WebLogic Suite for Oracle Applications	180	39.60	18,000	3,960.00	54	11.88
Coherence Enterprise Edition for Oracle Applications	46	10.12	4,600	1,012.00	14	3.08
WebLogic Suite Options for Oracle Applications:						
BPEL Process Manager Option for Oracle Applications	92	20.24	9,200	2,024.00	27	5.94
SOA Suite for Oracle Middleware for Oracle Applications	240	52.80	23,000	5,060.00	72	15.84
Unified Business Process Management Suite for Oracle Applications	230	50.60	23,000	5,060.00	69	15.18
Application Management						
Application Management Pack for Oracle Fusion Applications	50	11.00	5,000	1,100.00	15	3.30
WebCenter Products						
WebCenter Portal for Oracle Applications	350	77.00	50,000	11,000.00	105	23.10
WebCenter Imaging for Oracle Applications	368	80.96	36,800	8,096.00	110	24.20
Identity Management Product						
Identity and Access Management Suite Plus for Oracle Applications	9	1.98	80,000	17,600.00	9	1.98
Business Intelligence Technology Products						
Business Intelligence Publisher for Oracle Applications	60	13.20	18,400	4,048.00	18	3.96
Business Intelligence Suite Foundation Edition for Oracle Applications	500	110.00	180,000	39,600.00	150	33.00
Business Intelligence Suite Extended Edition for Oracle Applications	267	58.74	85,000	18,700.00	80	17.60

Figure 1 — Oracle products price Lists

2. Describe the concepts of Freemium.

FREEMIUM:

Freemium is a business model that works by offering a product or service free of charge (like software, web services etc) while charging a premium for advanced features and functionality.

What is the advantage of Cloud Computing Freemium Model versus the traditional way

Traditionally, the software or the content had to be downloaded by the End user. As the software is being installed on his / her computer by the End User, often some keygen are being used to unlock them.

As in case of most Cloud Computing based applications – that is SaaS, the real software is on the provider's server and protected efficiently from being misused by using various technologies, a trial is fully trial in when offered through Cloud Computing infrastructure.

Current approaches of Freemium model in Cloud Computing:

Full access and usage for a limited period, often the user needs to verify the Credit card. Rackspace Cloud and Amazon ECS can be the examples of Freemium model in Cloud Computing.

- Limited by the Capacity or the Features – Think of Free Cloud Storage and Free Apps offered by Google.

- Pay as you go in various cloud computing services is not really a Freemium model, but significantly reduces the cost.

Conclusion on Cloud Computing Free Model

Cloud Computing, itself has given various flexible opportunities to offer various software and services for free of cost.

- Unlike traditional way, Freemium model can be effectively controlled on the Cloud Computing infrastructure by the providers.
- Cloud Computing platform is suitable for pay as you go model – which is itself very convenient for the users.
- Indirectly, *Cloud Computing Freemium Model* can stop Software piracy – no one will use a pirated Microsoft office as Google Docs is available for free.
-

3. Explain in detail about the cloud cost management.

Cloud Cost Management:

Cloud cost management is an organizational practice that helps businesses understand and manage the costs and requirements associated with cloud technologies. Its main goal is to find more efficient cost-effective ways to use the cloud.

Cloud infrastructure is becoming more complex and as a result, cloud costs are difficult to track, visualize, and predict. The pay-as-you-go pricing model used by most public cloud providers makes this problem worse, because spend can fluctuate dramatically depending on the actual resources being used.

The Importance of Cloud Cost Management:

Cloud computing offers major advantages, including rapid scalability and the elimination of upfront capital investments. Cloud solutions allow DevOps and IT teams to start using services quickly and easily, but they also introduce a risk of unexpected costs that exceed your planned budget. You can implement a cloud cost management approach to help plan your organization's future cloud service consumption and costs.

Most companies today use multi-cloud deployments, making it especially important to establish an effective cost management strategy for the multi-cloud. This involves monitoring and comparing the costs of different cloud providers. Having deep visibility into your cloud usage and costs is essential for enforcing accountability across the organization, improving the performance of cloud-based

technologies, and informing decisions about the workloads running in each cloud environment.

Cloud cost management also helps you optimize resources to make the most of them. Public cloud providers usually offer a cost management tool to help you achieve this. However, specialized third-party cost management solutions offer greater visibility and insights into cloud costs, allowing you to control spending and implement good governance practices.

Cloud Cost Management vs. Cloud Cost Optimization:

Cloud cost management involves allocating and tracking cloud resources to analyze and report cloud spending. Cloud cost optimization takes these insights to help you understand how to minimize costs while maximizing business value.

Cloud cost optimization is not limited to cost savings—aligning costs with business goals is also important. When revenue increases, increasing costs might not be an issue.

Cloud cost growth often relates to indicators such as introducing new customers and launching new features. However, these activities usually bring higher returns. In software-as-a-service (SaaS) environments, higher revenues often lead to higher profit margins and help attract investors.

Cloud Cost Models:

Given the volatility of supply and demand, cloud offerings usually have dynamic cost models. A cloud cost model can be time-based, cost-based, or auction-based, depending on several factors.

The three main cloud pricing approaches are value-based, market-based, and fact-based. Demand drives value-based costing, supply drives fact-based costing, and supply-demand balance drives market-based costing.

Many people are unaware of the many unique pricing structures available with cloud computing. Understanding the different pricing options is important for models choosing the right cloud cost model and determining how the CSP bills you. Three main factors determine the cost of cloud computing services.

- **Compute**—most cloud service providers (CSPs) offer different compute instances with different memory and CPU features. They can also use specialized hardware such as high-speed networking and graphics acceleration. You pay based on each instance's number, type, and usage duration.

- **Network—**most CSPs charge based on the amount of data transferred to or from the cloud service. Additional fees for virtualized network services like static IP addresses, gateways, and load balancers may apply.
- **Storage—**CSPs offer storage-as-a-service options. For example, an elastic storage service may charge monthly for each GB of storage used. You pay for the entire storage volume of a managed storage service, such as a managed disk attached to a compute instance.

Here is an overview of the main cloud cost models.

Upfront Payment and Static Savings Plans:

A flat rate or upfront payment is a good option if you know your customers' level of demand in advance. Most cloud vendors are willing to negotiate discounted upfront rates if you commit to a certain usage amount or contract term.

Large enterprises that manage to negotiate discounts may choose a fixed payment method called Reserved Instances (RIs). They commit long-term to purchase a specified number of instances, guaranteeing a static service level at a fixed price.

Although the initial cost is high, the upfront payment model is the most predictable and transparent cloud cost option. If you can afford to spend a large part of your budget at once, you may save money in the long term. Learn more in our detailed guide to cloud cost savings (coming soon)

Pay-per-use Plans for Dynamic Cloud Services:

Paying a fixed price for cloud computing resources is not always viable if future demands are uncertain. You don't want to overpay for resources you might not need.

A pay-per-use plan may be better if your business has evolving demands. If your organization is likely to under-utilize cloud services for your customers, it makes more sense to pay for the resources you use rather than forecasting usage in advance.

Although you pay more per instance and miss out on a savings plan's discounts, a pay-as-you-go plan may deliver better overall savings. Because the charges match your real-time demands and usage, you can avoid paying for unused reserved instances.

What Are the Challenges of Cloud Cost Management?

Here are the main challenges of cloud cost management.

Insufficient Visibility into Your Cloud Spending:

A major cloud cost management challenge is a lack of visibility into a company's spending activities. Some businesses may encounter hidden costs because they lack the tools to track their cloud spending. You may end up spending more than necessary due to misunderstanding cloud costs.

You can solve this problem by granting access to cloud spending reports so that everyone can understand the impact of their activities on the company's spending. You can also use software with detailed visualizations that give you better insight into your cloud spending.

You can find and eliminate hidden costs associated with cloud services with the right cloud management tools. To manage your cloud costs, choose a tool that provides a comprehensive view of all the cost centers in the cloud. Aggregating all usage and cost reports helps you optimize your cloud costs.

Inaccurate Predictions and Budgets:

Cloud spending is difficult to predict, especially when using many cloud resources. Cloud costs can quickly increase when you adjust your roadmap or perform certain tasks.

Inaccurate budget forecasting can negatively impact your cloud cost management efforts. If your budget is too tight, you risk the application's performance. Going over budget could mean paying for resources you don't use. Don't rely on estimates alone—use a test environment to predict your future usage patterns.

A cloud cost management tool can analyze resource health to provide more accurate forecasts. It tells you what to expect based on historical data and trends.

Billing Complexity:

Billing can be complex and should not be the sole responsibility of the finance team. When building your cloud workloads, you must make sure every department understands its cloud costs. For example, development teams often focus on speed and efficiency and forget to manage cloud costs. Chargebacks must be transparent to prevent billing issues.

Cloud Cost Management Tools from the Leading Cloud Providers

AWS Cost Management Tools :

Amazon Web Services' cost management tools include:

AWS Cost Explorer:

Cost Explorer has a user-friendly interface to help customers view, analyze, and manage their AWS usage and costs over time. It offers several default reports that can be a starting point for cost analysis.

AWS Cost Categories:

The Cost Categories feature is part of the AWS Cost Management suite. It lets customers group usage and cost data into semantic categories based on their specific requirements. It supports custom categories that display cost-related information based on predefined rules, referencing dimensions like account, service, tag, and charge type.

AWS Budgets :

The Budgets feature lets customers create budgets for tracking their usage and costs across various use cases. It supports SNS and email notifications to alert customers when costs approach or exceed the specified budget thresholds. Alerts can also indicate if Savings Plan coverage falls below the specified threshold.

AWS Cost and Usage Reports (CURs):

A CUR contains detailed AWS usage and cost information. They contain added metadata about reserved instances, savings plans, services, credit, pricing, fees, discounts, and taxes. It itemizes AWS usage based on usage type, product, and operation at the organization or account level. CURs are available at the member or management account levels and at monthly, daily, or monthly levels of granularity.

4. Describe the cloud cost models.

Cloud Cost Models

Here are several common cost models used in the cloud, which you can combine depending on your needs.

Pay-As-You-Go

In this model, cloud services are billed per actual usage. Cloud services may bill for utilization of computing power, storage, networking, or other resources. The advantage is that you only pay for actual usage, and can scale down resources when needed. The downside is that as you add more resources to your cloud deployment, ongoing costs can quickly skyrocket.

Prepaid/Fixed Subscriptions

In a subscription-based model, cloud customers pay for services upfront. Subscription prices deliver a predetermined package of services for a specified time. The longer the period, the lower the price.

Subscription pricing is common for cloud services that combine multiple hardware and software elements, like platform as a service (PaaS) and software as a service (SaaS). Most cloud providers also offer subscription-based pricing for customers with high spend, allowing them to enter into a corporate discount plan, where they commit to a certain level of cloud spend and receive a discount on some or all of their cloud services.

Reserved Instances

Reserved instances allow companies to commit to cloud resources for a long period of time, typically 1 or 3 years. The longer the discount, and the more the company is prepared to pre-pay at the beginning of the period, the greater the discount. A three-year term is usually the most cost effective. Cloud providers typically offer discounts of 50-75% compared to pay-as-you-go rates for reserved instances with the same capabilities.

Reserved instances are suitable for steady state loads and long running systems. However, organizations should not use reserved instances for peak loads. Instead, reserved capacity should be used for core components of the system, and additional capacity required during peaks should be handled using pay-as-you-go or spot instances (see below).

AWS Savings Plan

Similar to reserved instances, Savings Plans are a flexible pricing model that allows organizations to enjoy lower than on-demand pricing, in exchange for a one-year or three-year specific usage commitment. The commitment is expressed in terms of spend per hour on Amazon services.

AWS offers three types of Savings Plans:

- **Compute Savings Plans** – apply to all usage of Amazon compute services usage, including EC2, AWS Lambda and Fargate.
- **EC2 Savings Plans** – applies only to usage of Amazon EC2 instances.
- **SageMaker Savings Plans** – applies only to SageMaker usage.

Savings plan offer three payment methods:

- **No upfront** – does not require an upfront payment, bills customers according to actual usage each month. This grants the minimal savings plan discount.

- **Partial upfront payment** – with this option, more than half of your contract is prepaid and the rest is billed monthly, which grants an additional discount.
- **Full upfront payment** – the full commitment is paid upfront, which grants the deepest discount.

Spot Instances

Spot instances are usually the lowest-cost computing option, offering discounts of up to 90% compared to pay-as-you-go rates. Spot instances are used by cloud providers to sell off spare capacity. The discount comes with a catch—spot instances can be interrupted at very short notice.

Ordinarily, spot instances can only be used for workloads that are stateless, fault tolerant, or processes that can be stopped and restarted. Cloud optimization technology like Elastigroup from Spot by NetApp can help you leverage spot instances for demanding, mission critical workloads as well.

Learn more in our detailed guide to cloud cost models

5. Explain in detail about the Opex and capex.

CapEx In Cloud Computing:

CapEx is short for capital expenditure. **Capital expenditure is the cost a business incurs to acquire assets that will provide benefits beyond the current year.** CapEx is also referred to as PP&E, which stands for Property, Plant, and Equipment.

When a company invests money, uses collateral, or incurs debt in order to acquire new assets or increase their value over time, they incur capital expenditures. So, capital expenditures are usually long-term investments in the business.

Also, CapEx IT spending is often a one-time purchase of a specific high- dollar fixed asset during a single tax year, with little ongoing costs during that period.

Examples of CapEx expenditure in the cloud:

- Building/premises purchase
- Physical data center equipment like servers and networking infrastructure
- IT equipment for IT and office staff
- Patents
- Installing local software or in-house applications

- Datacenter renovation
- Restoring an asset's value through upgrades
- Repurposing an asset
- Setup and supporting infrastructure costs
- Repairs beyond routine maintena

Characteristics of CapEx expenditure:

The key to determining capital expenditure is to observe distinct concepts, such as where they should be accounted for and how they should be taxed. Here's how.

- **Long-term** - Procured to provide benefits past the current tax year. Many assets, such as buildings, patents, and computers, remain economically viable for decades.
- **Approval** - The process involves a lot of long-term planning, including forecasting future demand versus potential returns in advance. So, CapEx-based IT spending often takes a lot of time to approve.
- **Ownership** - Once you clear the payment, you take full ownership of the tangible or intangible asset. You can finance the purchase with debt, savings, or retained profits.
- **Responsibility** - As the owner of the asset, you are in charge of all aspects of it, such as security, updates, upgrades, repairs, maintenance, and training employees. In addition, you decide who, what, and why to use the asset.
- **Upfront cost** - You pay for them in advance — before using them. Most CapEx projects are one-time investments, only requiring updates, upgrades, or replacements every five to ten years.
- **High-ticket** - Capital expenditure often covers assets, which can be costly to acquire but are essential for starting, running, and maintaining a business.
- **On-premises** - Most CapEx spend is often for physical, fixed assets that you will install, run, and maintain on-premises or within a physical data center.
- **Tax treatment** - Intangible assets are amortized over time, whereas physical assets are depreciated over their lifetime. So, you do not claim CapEx costs in their entirety the same year you incur them.

Financial reporting - While some capital expenditures are fully expensed the same year you make them, they usually go into the balance sheet as assets, not expenses. Only a percentage of it goes on the profit and loss statement (as a depreciation expense on an ongoing basis).

UNIT-V: CLOUD SERVICE GOVERNANCE AND VALUE

IT Governance Definition- cloud governance definition-cloud governance framework-cloud governance structure-cloud governance-considerations-cloud service model-Risk matrix-understanding value of cloud service-measuring the value of cloud services- Balanced scorecard- **Total cost ownership.**

PART-A:

1. **What is meant by IT goverence?**
2. **Why is IT governance important?**
3. **What is corporate governance?**
4. **Define COBIT.**
5. **What Is Cloud Governance?**
6. **List out the Cloud Governance Benefits.**
7. **What are the steps needed to setting up a cloud Governance Framework?**
8. **What are the objectives for cloud security?**
9. **What are the principles of cloud governance model?**
10. **Define TCO.**
11. **Define Cloud zero.**

PART-B:

1.Explain in detail about the IT Governance.
2.Describe the concepts of cloud governance.
3.Explain in detail about the TCO.

PART-A:

1. What is meant by IT goverence?

IT governance is an element of corporate governance, aimed at improving the overall management of IT and deriving improved value from investment in information and technology.IT governance frameworks enable organisations to manage their IT risks effectively and ensure that the activities associated with information and technology are aligned with their overall business objectives.

2. **Why is IT governance important?**

IT governance enables an organisation to:

- Demonstrate measurable results against broader business strategies and goals.
- Meet relevant legal and regulatory obligations, such as those set out in the GDPR (General Data Protection Regulation) or the Companies Act 2006.
- Assure stakeholders they can have confidence in your organisation's IT services.
- Facilitate an increase in the return on IT investment; and
- Comply with certain corporate governance or public listing rules or requirements.

3. What is corporate governance?

Corporate governance *is* "a toolkit that enables management and the board to deal more effectively with the challenges of running a company. Corporate governance ensures that businesses have appropriate decision.

4.Define COBIT.

COBIT (Control Objectives for Information and Related Technology) is an internationally recognised IT governance control framework that helps organisations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organisational goals.

5. What Is Cloud Governance?

Cloud governance is a set of policies and rules used by companies who build or work in the cloud. This framework is designed to ensure data security, system integration and the deployment of cloud computing are properly managed

6. List out the Cloud Governance Benefits.

- Improves management of resources so there is no overlap for different teams working separately in the cloud.
- Improves cloud security issues by having comprehensive rules and protections in place designed to thwart cybercriminals.
- Helps curb shadow IT — the use of applications, software and services without approval from the IT department.
- Reduces administrative overhead and labor when cloud computing follows the same rules across your entire business.

7. What are the steps needed to setting up a cloud Governance Framework

There are three steps involved in setting up a cloud governance framework for your business.

1. Define Controls:
2. Implement Controls
3. Audit Controls

8. What are the objectives for cloud security

- Enable cost management by developing a strict process for determining real cost savings.
- Create a governance team to ensure teams across your business are following the framework.
- Establish programmatic controls for automating processes and establishing security protocols.

9. What are the principles of cloud governance model.

1. Compliance with policies and standards
2. Alignment with business objectives
3. Collaboration
4. Change management
5. Dynamic response

10. Define TCO.

The total cost of ownership in cloud computing refers to the total cost of adopting, operating, and provisioning cloud infrastructure.

11. Define Cloud zero.

CloudZero is a cost intelligence platform that enables a deep understanding of your cloud unit economics and provides a continuous feedback loop to your engineering team while you migrate.

PART-B:

1.Explain in detail about the IT Governance.

IT governance definition:

IT governance is an element of corporate governance, aimed at improving the overall management of IT and deriving improved value from investment in information and technology.

IT governance frameworks enable organisations to manage their IT risks effectively and ensure that the activities associated with information and technology are aligned with their overall business objectives.

Important of IT governance:

IT governance enables an organisation to:

- Demonstrate measurable results against broader business strategies and goals.
- Meet relevant legal and regulatory obligations, such as those set out in the GDPR (General Data Protection Regulation) or the Companies Act 2006.
- Assure stakeholders they can have confidence in your organisation's IT services.
- Facilitate an increase in the return on IT investment; and
- Comply with certain corporate governance or public listing rules or requirements.

Corporate governance:

Corporate governance is *"a toolkit that enables management and the board to deal more effectively with the challenges of running a company. Corporate governance ensures that businesses have appropriate decision-making processes and controls in place so that the interests of all stakeholders are balanced."*- ICSA, The Governance Institute.

A robust corporate governance framework can help you meet the requirements of laws and regulations such as the DPA (Data Protection Act) 2018 and the GDPR.

For instance, the GDPR requires data controllers and processors to demonstrate their compliance with its requirements through certain documentation, including relevant logs, policies and procedures.

Harnessing the elements of IT governance will help you create and maintain appropriate policies and procedures to help meet your data privacy requirements.

IT governance frameworks, models and standards:

ISO 38500 – The international IT governance standard:

ISO/IEC 38500:2015 is the international standard for corporate governance of IT.

It sets out principles, definitions and a high-level framework that organisations of all types and sizes can use to better align their use of IT with organisational decisions and meet their legal, regulatory and ethical obligations.

Buy a copy of ISO/IEC 38500:2015

As well as ISO 38500, there are numerous widely recognised, vendor-neutral frameworks that organisations can use to implement an IT governance programme. Each has its own IT governance strengths – for instance, COBIT focuses more on process management and ITIL on service management – but you might benefit from an integrated approach, using parts of several frameworks to deliver the results you need.

Follow the links below to find out more about each framework.

ITIL – IT service management:

Widely adopted around the world, ITIL is a framework for ITSM (IT service management). Its latest iteration, ITIL 4, was launched in February 2019.

ITIL is supported by ISO/IEC 20000-1:2018 – the international standard for ITSM against which organisations can achieve independent certification.

Learn more about ITIL

Browse ITIL products

COBIT:

COBIT (Control Objectives for Information and Related Technology) is an internationally recognised IT governance control framework that helps organisations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organisational goals.

COBIT 2019, the latest iteration of the framework, was released in November 2018. It builds on COBIT 5, introducing new concepts and addressing the latest developments affecting enterprise IT.

Calder-Moir IT Governance Framework:

framework provides structured guidance on how to approach IT governance. It can help benchmark the balance and effectiveness of IT governance practices within an organisation.

The IT Governance Control Framework Implementation Toolkit provides practical assistance and guidance for practitioners and board members tackling the subject.

The five domains of IT governance:

The IT Governance Institute (a division of ISACA) breaks down IT governance into five domains:

1. Value delivery
2. Strategic alignment
3. Performance management
4. Resource management
5. Risk management

Other IT governance frameworks and models to consider

In addition to the frameworks listed above, there are several other models and frameworks you should consider for effective IT governance:

- King reports of corporate governance (versions I to IV).
- ISO/IEC 31000:2018 (risk management).
- ISO/IEC 27001:2013 (information security).
- Business continuity management and disaster recovery.
- Knowledge management, including intellectual capital.
- Programme management and project governance, including PRINCE2® and PMBOK®

.

2.Describe the concepts of cloud governance.

Cloud Governance:

- **It is the set** of polices or principles that act as the guidance for the adoption use, and management of cloud technology services.
- It is an ongoing process that must sit on top of existing governance models.
- It is a set of rules you create to monitor and amend as necessary in order to control costs, improve efficiency,and eliminate security risks.

Cloud governance is a set of policies and rules used by companies who build or work in the cloud. This framework is designed to ensure data security, system integration and the deployment of cloud computing are properly managed. Since

cloud systems are dynamic, involving third-party vendors or different teams within your business, cloud governance solutions must be adaptable.

A cloud governance framework done right will manage risks, enhance data security and enable cloud systems operations for your business. This method of cloud computing governance for IT balances resource and risk with a focus on accountability. Without cloud governance you run the risk of poor integration of cloud systems and a lack of alignment with business goals and face new security issues associated with deploying cloud systems.

Cloud Governance Benefits:

A good cloud governance framework can provide your business with the following benefits:

- Improves management of resources so there is no overlap for different teams working separately in the cloud.
- Improves cloud security issues by having comprehensive rules and protections in place designed to thwart cybercriminals.
- Helps curb shadow IT — the use of applications, software and services without approval from the IT department.
- Reduces administrative overhead and labor when cloud computing follows the same rules across your entire business.

Whether your business uses the public cloud or private cloud, cloud security provided by cloud computing governance is vital. Ensuring that your business aligns with the principles of cloud governance is a step toward smooth cloud operations.

Setting Up a Cloud Governance Framework

There are three steps involved in setting up a cloud governance framework for your business.

1. **Define Controls**: Define your controls, both financial and operational. This can involve following regulatory rules such as HIPAA, limiting the number of cloud instances you use and deciding who has clearance to make changes to your cloud computing environment.
2. **Implement Controls**: Once you have a policy document defining the rules to fit your business needs, implement those controls. Communicate with teams and employees and optionally use third-party tools to help you implement controls.
3. **Audit Controls**: Continuously monitor controls to make sure you are doing all the right things the right way and monitoring them the right way.

Cloud Governance Implementation Challenges:

While considering these principles and taking the steps to set up cloud governance, it is important to understand the challenges associated with implementation.

The three most common challenges of implementing a cloud governance framework are cloud adoption, governing data in the cloud, and cloud security. Keeping these challenges in mind, you can implement cloud governance for your business in an effective manner.

Cloud Adoption:

The challenges for a business newly adopting cloud computing include skill gaps, existing data center investments, and vendor lock-in. Training your teams to be skilled in the cloud is an important step to take before adopting cloud computing. Understanding your business costs and the process of migrating from on-premises data centers to the cloud is also vital. Some third-party vendors will lock your business in, meaning you won't be able to easily swap vendors once you start building with them.

You may also find challenges with management buy-in or a lack of metrics for measuring performance and risk. Credential and access management, insufficient identity protocols, and security teams not versed in the cloud can all affect your business security. It is important to embed management controls into your operations and create operating models to alleviate these risks and challenges.

Governing Data in the Cloud:

Governing data in the cloud also has challenges related to information security. Following regulations for the types of data your business uses is an important aspect of your data governance framework. It is important to understand the needs of your business and the laws surrounding cloud data governance. If your business follows along with best practices, you can help your business thrive using cloud governance.

Cloud Security:

Because of the unique nature of the cloud environment, many of the challenges associated with cloud governance are cloud security challenges like data breaches and system vulnerabilities. Building a strong cloud security strategy is an essential component to keeping your organization's cloud environments safe from adversaries.

3.Explain in detail about the TCO.

TCO:

Total cost of ownership (TCO) is the sum of all costs involved in the purchase, operation, and maintenance of a given asset during its lifetime. TCO helps businesses understand the cost of a tool beyond the initial purchase price and is extremely helpful for understanding ROI.

The total cost of ownership in cloud computing refers to the total cost of adopting, operating, and provisioning cloud infrastructure. Organizations often find it necessary to perform a cloud TCO analysis when they are considering moving to the cloud because it allows them to weigh the cost of cloud adoption against the cost of running their current on-premise systems.

While this is a good place to start, you may not get the full picture. This is because a head-to-head comparison does not capture hidden costs or intangible costs of not switching to the cloud (i.e. the benefits of a cloud solution), such as faster time to market, increased productivity, and elasticity of demand.

To accurately calculate cloud TCO, you must capture not only the purchase price of on-premises vs. cloud solutions but also the intangible costs associated with either solution.

In this article, we'll discuss the best approach and practices when evaluating the total cost of ownership for cloud computing.

Steps For Calculating Cloud TCO:

Below are some of the steps you should follow when estimating cloud total cost of ownership.

Step 1: Calculate your current IT infrastructure costs:

Understanding the actual cost of your current IT solution is the first step. This means calculating the direct and indirect costs of running and maintaining your current system as well as estimating your current workloads, including servers, databases, storage, and network bandwidth.

Consider the following cost areas:

- **Hardware and infrastructure—**Identify the cost of the hardware that powers your on-premise application. These include physical servers, supplies, spare parts, etc.
- **Datacenter**—How much does it cost to power your data center? How much does it cost to meet your current cooling, power, and space requirements?

- **Software**—Calculate your current software usage, including the number of licenses and cost of these licenses.
- **Personnel**—Identify all the personnel involved in system, network, and database administration and how much it costs to payroll them.
- **Disaster recovery**—If you have a disaster recovery system in place, how much does it cost to maintain and manage that site?
- **Maintenance**—Calculate the cost of servicing, operating, and maintaining the system, including the cost of both in-house and outsourced maintenance.
- **Upgrades**—How much will it cost to upgrade the system if the need arises? Would you need to overhaul the system completely?
- **Security**—Estimate the total cost of securing your current system, from the cost of physical security to firewalls and security experts.
- **Hidden costs**—How much does downtime cost you? Review log files to determine server downtime frequency, hours lost, and the cost implication of those hours.

Two of the major cost areas to consider for the cloud are **migration costs** and the **monthly cost of your selected cloud services.**

1. Migration costs:

Moving your applications and data to the cloud is a key step when switching to the cloud. Your current applications may require modification to function properly in the cloud. Gartner identifies the five ways to move applications into the cloud, namely:

- Rehosting applications without making any changes to their architecture
- Refactoring or running applications on a cloud provider's infrastructure
- Revising the application, i.e. modifying or extending the existing code base
- Rebuilding or rearchitecting the entire application for the cloud
- Replacing the application with commercial software delivered as a service

Each application migration method has its cost implications and you need to determine the costs associated with the method you choose. In addition to application migration costs, estimate data transfer charges that will accrue when moving your application.

2. Monthly cloud cost:

Your monthly cloud cost will depend on your workloads, and the specific cloud services consumed and method of purchase. The goal here is to estimate your potential monthly cloud bill based on your current workloads.

Since this calculation differs considerably for each organization, major cloud platforms provide pricing calculators that make it easier to estimate your monthly cloud bill. The AWS pricing calculator, for example, allows you to estimate your infrastructure cost based on the retinue of AWS products and services selected.
Two of the major factors that will affect the size of your cloud bill are:

Type of cloud services consumed:

Commodity services, such as storage or raw compute power, are relatively less expensive compared to more specialized services, such as machine learning. Amazon, for instance, offers Rekognition which does image and video analysis, and Polly, which is a text-to-speech service. These services have higher workload costs than storage. The total cost will depend on the types of services your business needs.

Cloud consumption model:

The on-demand model, where resources are deployed as needed, is the most popular cloud usage model. However, it is also the most expensive cloud consumption model. The other way to consume cloud services is to use a savings plan or prepaid option (reserved instances). You could also opt for a hybrid model. Your cloud costs will differ depending on the consumption model your business adopts.

3. Consultation and training costs:

If your team lacks the expertise required for the migration process, factor in the cost of hiring consultants for training.

Step 3: Consider the intangible benefits of the cloud:

Beyond comparing the monetary implications of on-premise versus cloud solutions, there are opportunity costs associated with *not* switching to the cloud. You need to quantify what this means for your business.

Innovation—The cloud offers hundreds of services you can access on demand. By continuing with an on-premises system, you sacrifice the ability of developers to move fast and respond quickly to market changes.

Elasticity—Handling demand in an on-premise environment is always a challenge. The solution is usually to maintain redundant infrastructure in anticipation of peak loads. In the cloud, however, you could easily deploy instances to take care of the additional peak without any downtime.

When the peak is over, you go back to operating at your normal capacity at no additional cost. While you may incur a larger monthly cloud bill at peak, you will experience no downtime nor would you need to maintain redundant infrastructure when the surge is over.

Comparing On-Premise TCO To Cloud TCO:

At the end of your cloud TCO analysis, you should have specific numbers that can help with your decision-making. A few things should guide understanding of the results:

1. Cloud computing is not inherently cheaper than an on-premise model.
2. Cloud adoption is rarely about pure cost savings. Often the end result is a larger ROI and better business outcomes, not lower TCO, even though it could be both.
3. Comparing the business value and opportunity cost of switching to the cloud versus using an on-premises model is just as important as comparing head- to-head costs.
4. Identifying cost savings and efficiencies is critical when performing a cloud TCO analysis.