Unit-2

**Why Migrating To the Cloud? Benefits You Might Have Not Considered**

## What can be migrated to a cloud?

**Cloud migration is the process of moving a company’s digital assets, services, databases, IT resources, and applications either partially, or wholly, into the cloud. Cloud migration is also about moving from one cloud to another.**

Cloud migration is a process in which digital resources are moved from on-premise infrastructure to a cloud. You can do it even with your holiday photos. In business, however, there are three main situations when you will benefit from such a migration. First, you may want to move your data-sources to a cloud. Databases, shared files, etc. When more people need to work on the same data or files, it’s tempting to migrate them. Profits? Flexibility, mobility, and security.

Second, you may move whole applications used in your company to a cloud as well. Although not every application can get installed and used that way, it’s becoming more and more popular. It’s great for many reasons including lower maintenance costs and higher flexibility.

The third one happens when it is your company that provides software. You can then use dedicated services, platforms, and ready-to-use components, to create a cloud-based application. Such an app will benefit from the cloud computing advantages and improve your customers’ UX.

Importantly, you don’t always need or have to migrate all your resources to a cloud. For some reason, it’s often advisable to keep some crucial data inside. Moreover, depending on how your company works and what are your development plans you should decide, which processes will benefit most from the migration, and which don’t need it at all. It’s even possible to design and create an ecosystem consisting of both your on-premise infrastructure and a cloud. Choosing the right combination will let your company experience the vast pool of benefits of cloud computing.

So, what are these benefits?

## What are the benefits of cloud migration

Before deciding on migrating your assets to a cloud, consider the benefits. Will they apply to your business? Look at the list of cloud migrations benefits below to find out, how this process may influence the way you work.

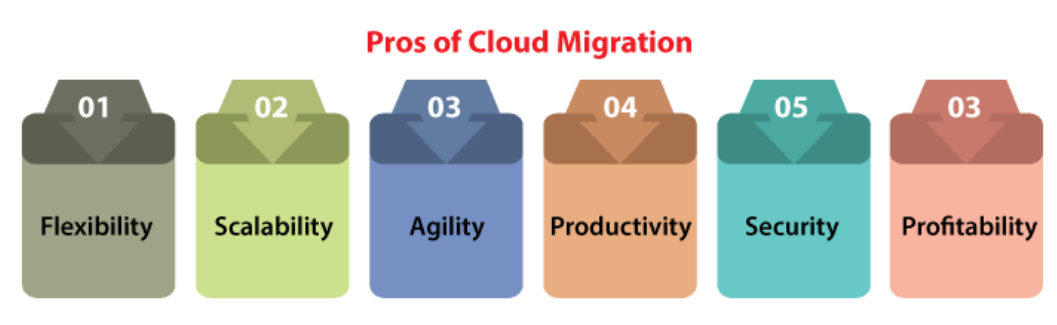
* **Scalability** – it is much easier to grow and to keep (and improve) the quality of your work when using cloud-based solutions. Moreover, it is then your cloud provider business to prepare their infrastructure for your growth. What’s even better is that your cloud can adjust the level of assets needed for the amount of traffic you’re exposed to. In other words, clouds make it possible that scalability happens instantly.
* **Reliability** – together with better scalability, comes the higher reliability. Clouds are designed in such a way, that they (almost) always are accessible and ready to work. As a cloud user, you don’t rely on one server or data-center only. As a result, you can count on incredibly high SLA, sometimes reaching 100% accessibility!
* **Disaster recovery and automatic backup** – help you ensure that nothing vanishes in case of any breakdown. Clouds are almost data-loss resistant because store copies of data in multiple locations.
* **Security** – previous points also add up to the security benefit. However, there’s more to this. Cloud providers usually have access to better, more breach-resistant security solutions as well as experts. What’s more, as their customer, you’re not alone regarding security and software updates. Cloud providers usually offer the so-called Shared Responsibility Model, in which the responsibility for maintenance and security is divided between the customer and provider.
* **Lower costs** – especially if you choose e.g. IaaS (Infrastructure as a Service) you will gain the ability to adjust the infrastructure and costs to your current situation and needs.
* **Improved monitoring and analytics** – cloud solutions often have built-in monitoring services. Together with automatic and standardized logging of the key metrics, you are equipped with access to the most reliable data bout your infrastructure and maintenance. Even better, most cloud providers offer e-mail or phone notifications about the state of your infrastructure, assets, or breakdown.
* **Improved IT resource management** – – when you want to change anything in your IT hardware, you need to find, buy, and assemble new parts (you, or your IT expert). When you are a cloud customer all you need to do is to choose proper components in Software as a Service or Infrastructure as a Service models. It smoothens your processes.
* **Increased mobility** – with a cloud it’s much easier (and more secure) to work remotely and in a move. It’s become even more vital after the outbreak of the COVID-19 pandemic. Increased mobility also means that moving your office is easier and makes your company more flexible.
* **Collaboration** – clouds make it easier to collaborate as well. Especially for remote teams with workers in different locations.
* **Reduced carbon footprint** – last but not least, thanks to the economies of scale, cloud providers are often greener and produce lower carbon footprint.

Summing up, cloud migration will help you enhance your business performance, improves your company scalability ensuring security at the same time. Moreover, it is a way to transform your company and make it more [**Agile**](https://blog.inspeerity.com/agile/how-software-development-can-be-agile/).

## **Pros of Cloud Migration**

Organizations migrate to a cloud for various reasons, but, normally when faced with many challenges of developing IT infrastructure within the most secure and cost-effective way possible.

Some of the advantages of migrating to a cloud are as follows:



* **Flexibility:** No organization facilitating experiences a similar demand level by a similar number of users every time. If our apps face fluctuations in traffic, then cloud infrastructure permits us to scale down and up to meet the demand. Hence, we can apply only those resources we require.
* **Scalability:** The analytics grow as the organization grows with databases, and other escalates workloads. The cloud facilitates the ability to enhance existing infrastructure. Therefore, applications have space to raise without impacting work.
* **Agility:** The part of the development is remaining elastic enough for responding to rapid modifications within the technology resources. Cloud adoption offers this by decreasing the time drastically it takes for procuring new storage and inventory.
* **Productivity:** Our cloud provider could handle the complexities of our infrastructure so we can concentrate on productivity. Furthermore, the remote accessibility and simplicity of most of the cloud solutions define that our team can concentrate on what matters such as growing our business.
* **Security:** The cloud facilitates security than various others data centers by centrally storing data. Also, most of the cloud providers give some built-in aspects including cross-enterprise visibility, periodic updates, and security analytics.
* **Profitability:** The cloud pursues a pay-per-use technique. There is no requirement to pay for extra charges or to invest continually in training on, maintaining, making, and updating space for various physical servers.

## **Cloud Migration Strategies Types**

Migrating to a cloud can be a good investment for our business. We might be admiring where to start like several companies.  
Gartner specified some options that are widely called "the six Rs of migration", defined as follows:



### **1. Rehosting (lift-and-shift)**

The most general path is rehosting (or lift-and-shift), which implements as it sounds. It holds our application and then drops it into our new hosting platform without changing the architecture and code of the app. Also, it is a general way for enterprises unfamiliar with cloud computing, who profit from the deployment speed without having to waste money or time on planning for enlargement.

Besides, by migrating our existing infrastructure, we are applying a cloud just like other data centers. It pays for making good use of various cloud services present for a few enterprises. For example, adding scalable functions to our application to develop the experience for an improving segment of many users.

### **2. Re-platforming**

Re-platforming is called "**lift-tinker-and-shift**". It includes making some cloud optimizations without modifying our app's core architecture. It is the better strategy for enterprises that are not ready for configuration and expansion, or those enterprises that wish to improve trust inside the cloud.

### **3. Re-factoring**

It means to rebuild our applications from leverage to scratch cloud-native abilities. We could not perform serverless computing or auto-scaling. A potential disadvantage is **vendor lock-in** as we are re-creating on the cloud infrastructure. It is the most expensive and time-consuming route as we may expect. But, it is also future-proof for enterprises that wish to take benefit from more standard cloud features.  
It covers the most common three approaches for migrating our existing infrastructure.

### **4. Re-purchasing**

It means replacing our existing applications along with a new SaaS-based and cloud-native platform (such as a homegrown CRM using Salesforce). The complexity is losing the existing training and code's familiarity with our team over a new platform. However, the profit is ignoring the cost of the development.

**Re-purchasing** is the most cost-effective process if moving through a highly personalized legacy landscape and minimizing the apps and service number we have to handle. Once we have accessed the nature and size of our application portfolio, we may detect cloud migration is not correct for us.

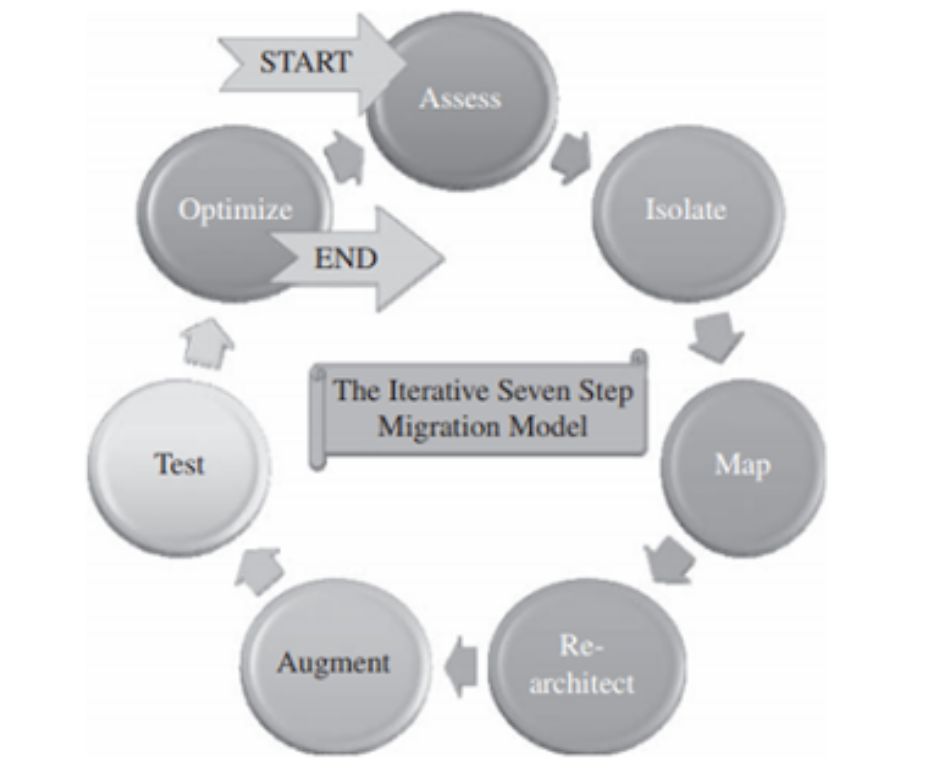
### **5. Retiring**

When we don't find an application useful and then simply turn off these applications. The consequencing savings may boost our business situation for application migration if we are accessible for making the move

### **6. Re-visiting**

Re-visiting may be all or some of our applications must reside in the house. For example, applications that have unique sensitivity or handle internal processes to an enterprise. Don't be scared for revisiting cloud computing at any later date. We must migrate only what makes effects to the business.

The seven step model of Migration into Cloud



**Step 1 ASSESSMENT**

* Cloud migration assessments comprise assessments to understand the issues involved in the specific case of migration at the application level or the code, the design, the architecture, or usage levels.
* These assessments are about the cost of migration as well as about the ROI that can be achieved in the case of production version.
* Moreover, assessments are also required for tools being used, functionality, test cases, and configuration of the application.
* The proof of concepts for migration and the corresponding pricing details will help to assess these issues properly.

**Step 2 ISOLATE**

* The second step is the isolation of all the environmental and systemic dependencies of the enterprise application within the captive data center.
* These include library, application, and architectural dependencies. This step results in a better understanding of the complexity of the migration.

**Step-3 MAP**

* A mapping construct is generated to separate the components that should reside in the captive data center from the ones that will go into the cloud.

**Step-4 RE-ARCHITECT**

* It is likely that a substantial part of the application has to be re-architected and implemented in the cloud.
* This can affect the functionalities of the application and some of these might be lost. It is possible to approximate lost functionality using cloud runtime support API.

**Step-5 AUGMENT**

The features of cloud computing service are used to augment the application.

**Step-6 TEST**

Once the augmentation is done, the application needs to be validated and tested. This is to be done using a test suite for the applications on the cloud. New test cases due to augmentation and proof-of-concepts are also tested at this stage.

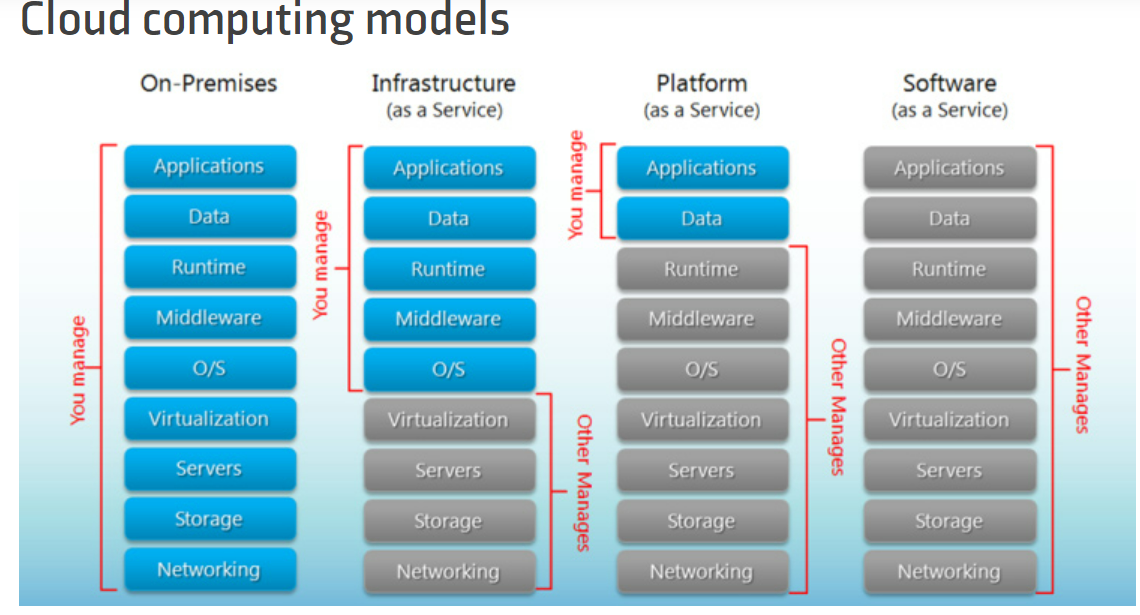
**Step-7 OPTIMISE**

The test results from the last step can be mixed and so require iteration and optimization. It may take several optimizing iterations for the migration to be successful. It is best to iterate through this seven step model as this will ensure the migration to be robust and comprehensive.

Migration Risks and Mitigation

An overview of the three kinds of cloud computing models (and the typical cloud migration challenges they create in migration) is an excellent place to start in the decision-making process.

* **IaaS** – Infrastructure as a Service (AWS, Azure, Google Compute Engine)
* **PaaS** – Platform as a Service (examples: AWS Elastic Beanstalk, Heroku, Google App Engine)
* **SaaS** – Software as a Service (examples: Google Apps, Salesforce)



According to Richard Watson of Gartner, “Choosing the optimal application-migration option is a decision that can’t be taken in isolation. Any cloud-migration decision is, in essence, an application or infrastructure modernization decision and needs to be approached in the broader context of related infrastructure and application portfolio management programs. This **decision is not solely an issue of cloud migration but of optimization**. Which cloud platform and migration techniques offer the chance to optimize the application’s contribution to stated and implied business and IT goals? Those business and supporting IT goals, described next, should be driving any cloud migration decision — not a rush to experiment with new toys.”

Furthermore, find the risks involved in cloud migration and mitigation strategies for each of them.

## **Cloud Migration Risks and Mitigation Strategies**

### **1. Intricate Architecture**

Cloud migrations approaches often fail due to the complex architecture. Data-rich applications are also dependent on multiple elements and environments.

Cloud Migration Strategy**: Manage** only one **complex architecture** that is currently**existing on-premise.** Design architecture in such a way that it consumes data stored in the enterprise’s IT environment.

### **2. Multiple Dependencies**

Multiple dependencies with on-premises environments create problems during lift and shift.

Cloud Mitigation Strategy: The best bet is to **consider solutions that test before migration.** They can identify and remediate the differences in environments. Seek the services of a cloud services provider who offers services that are relevant to your needs.

### **3. Data Gravity**

Data Gravity becomes difficult to test if an application and its data are not working as it should in the cloud. Most replication-based migration tools require data to be moved before the apps due to improper sequencing problems.

Cloud Migration Strategy: Use**live cloud migration approaches and tools** that stream the whole instance. Live migration eliminates the need for complex system synchronization and avoids consistency issues.

### **4. Management And Control Of Data Streams Within Heterogeneous Environments**

Databases that require a consistent view create unpredictable issues. Also, transactional production servers that continuously generate data are hard to manage. After data migration, the system must track and synchronize new changes to the production application. Furthermore, there may be security concerns with storing production data in the public cloud. It leads to a lack of control over multiple data repositories across a hybrid IT landscape.

Cloud Migration Strategy: Look for **solutions that offer secured connectivity**in the cloud, and implement them in a highly available configuration.

### **5. Cloud Gravity**



IT teams require workload mobility for effective data and workload migration. They must ensure these factors do not affect the business or introduce hidden costs.

Cloud Migration Strategy: In the case of data-rich enterprise applications, **evaluate migration solutions for speed and simplicity**. Enable portability and interoperability of stateless applications in a multi-cloud strategy, **using containers**.

### **6. Latency**

Applications can face latency issues when using cloud applications over the Internet.

Cloud Migration Strategy:  Use **optimization services** from a cloud service provider to help tide over latency issues.

### **7. Architectural difference**

It’s common to require modifications for your application design and architecture. But they may not be conducive for distributed cloud environments.

## **Cloud Computing Services**

## **What is cloud computing? What are the services offered?**

Cloud Computing is a process of delivering/enabling scalable, expandable and almost perfectly elastic software services using internet technologies. It is a method of delivering Software as a Service (SaaS), delivered in a pay-per-use basis. It provides self service capabilities to users with scalable features to increase usage on requirement.

The various cloud based services commonly offered are:

1. Web Based Cloud Computing: Companies use the functionality provided by web services and do not have to develop a full application for their needs.
2. Infrastructure as a Service (IaaS): Organizations make use of the unlimited storage potential of the cloud infrastructure. They can expand and shrink their storage space as needed without having to worry about dedicated servers on site.
3. Software as a Service (SaaS): It allows people to access the functionality of a particular software without worrying about storage or other issues.
4. [Platform as a Service (PaaS)](https://www.hcltech.com/technology-qa/what-is-paas): Companies can run their applications on the cloud service’s platform without having to worry about maintaining hard drives and servers.
5. Utility Services: Companies that need to store a lot of data can store all of their data remotely and can even create a virtual data center.
6. Managed Services: These are applications used by the cloud service providers, such as anti-spam service.
7. Service Commerce: It is the creation of a hub of applications that can be used by an organisation’s members. It provides organisations the applications they need along with the services they desire.

# Cloud Deployment Model

Today, organizations have many exciting opportunities to reimagine, repurpose and reinvent their businesses with the cloud. The last decade has seen even more businesses rely on it for quicker time to market, better efficiency, and scalability. It helps them achieve lo ng-term digital goals as part of their digital strategy.

Though the answer to which cloud model is an ideal fit for a business depends on your organization's computing and business needs. Choosing the right one from the various types of cloud service deployment models is essential. It would ensure your business is equipped with the performance, scalability, privacy, security, compliance & cost-effectiveness it requires. It is important to learn and explore what different deployment types can offer - around what particular problems it can solve.

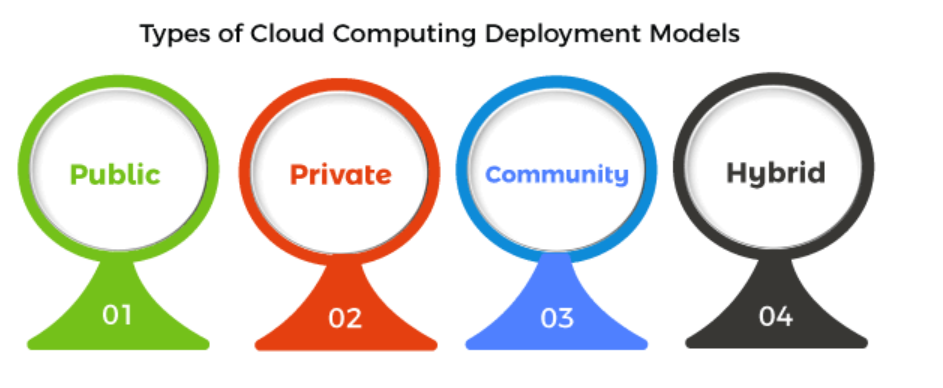
Read on as we cover the various cloud computing deployment and service models to help discover the best choice for your business.

### **What Is A Cloud Deployment Model?**

It works as your virtual computing environment with a choice of deployment model depending on how much data you want to store and who has access to the Infrastructure.

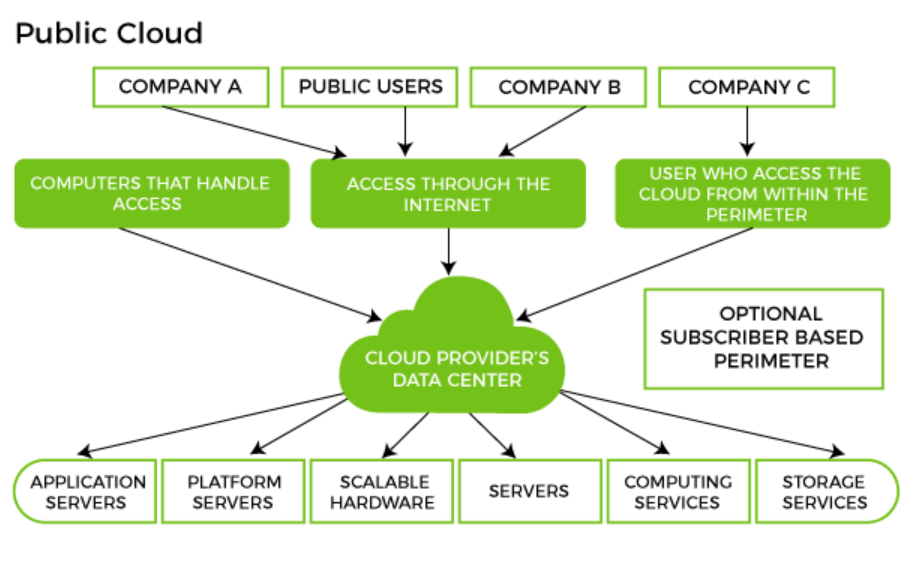
### **Different Types Of Cloud Computing Deployment Models**

Most cloud hubs have tens of thousands of servers and storage devices to enable fast loading. It is often possible to choose a geographic area to put the data "closer" to users. Thus, deployment models for cloud computing are categorized based on their location. To know which model would best fit the requirements of your organization, let us first learn about the various types.



### **Public Cloud**

The name says it all. 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. Thus, you pay a cloud service provider for networking services, compute virtualization & storage available on the public internet. 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.

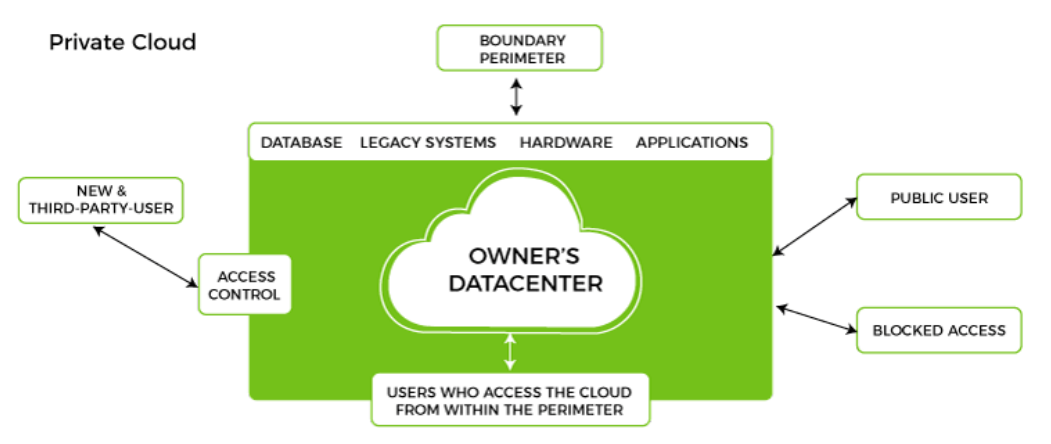
**Limitations of Public Cloud**

* 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**

Now that you understand what the public cloud could offer you, of course, you are keen to know what a private cloud can do. Companies that look for cost efficiency and greater control over data & resources will find the private cloud a more suitable choice.

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**

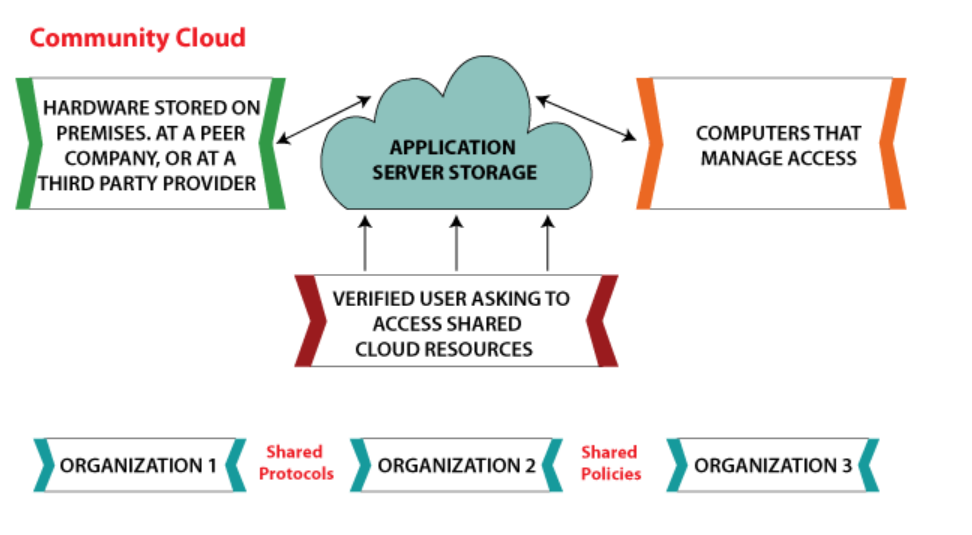
* Data Privacy - It is ideal for storing corporate data where only authorized personnel gets access
* Security - Segmentation of resources within the same Infrastructure can help with better access and higher levels of security.
* Supports Legacy Systems - This model supports legacy systems that cannot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

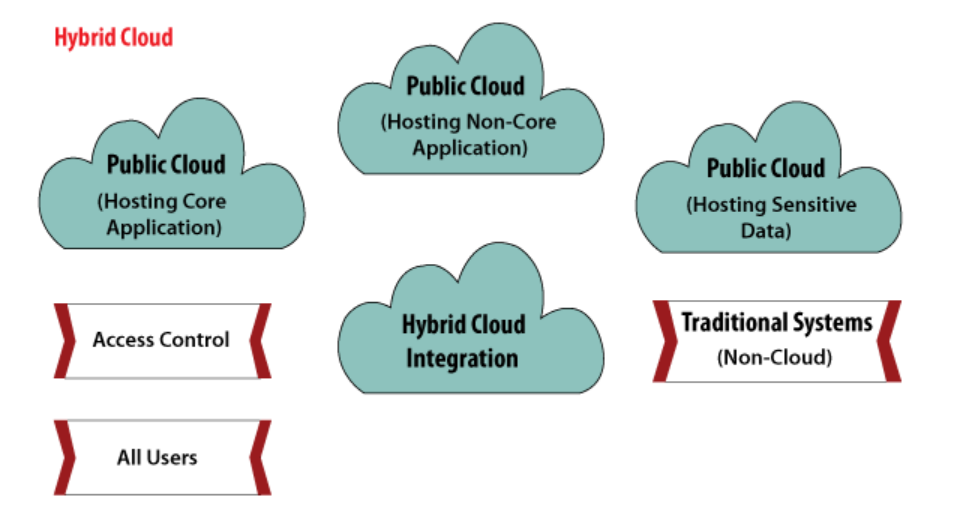
**Limitations of Community Cloud**

* 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**

As the name suggests, 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.

Let's understand the hybrid model better. 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:



# 7 Most Common Cloud Computing Challenges

Cloud computing is the provisioning of resources like data and storage on demand, that is in real-time. It has been proven to be revolutionary in the IT industry with the market valuation growing at a rapid rate. Cloud development has proved to be beneficial not only for huge public and private enterprises but small-scale businesses as well as it helps to cut costs. It is estimated that more than 94% of businesses will increase their spending on the cloud by more than 45%. This also has resulted in more and high-paying jobs if you are a cloud developer.

Cloud technology was flourishing before the pandemic, but there has been a sudden spike in cloud deployment and usage during the lockdown. The tremendous growth can be linked to the fact that classes have been shifted online, virtual office meetings are happening on video calling platforms, conferences are taking place virtually as well as on-demand streaming apps have a huge audience. All this is made possible by us of [**cloud computing**](https://www.geeksforgeeks.org/cloud-computing/) only. We are safe to conclude that the cloud is an important part of our life today, even if we are an enterprise, student, developer, or anyone else and are heavily dependent on it. But with this dependence, it is also important for us to look at the issues and challenges that arise with cloud computing. Therefore, today we bring you the most common challenges that are faced when dealing with cloud computing, let’s have a look at them one by one:

### 1. Data Security and Privacy

Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control. Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications. This can in turn lead to potential loss in revenue alongside reputation and stature. Also, dealing with cloud computing requires sending and receiving huge amounts of data at high speed, and therefore is susceptible to data leaks.

### 2. Cost Management

Even as almost all cloud service providers have a “Pay As You Go” model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing. When there is under optimization of the resources, let’s say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up. If you turn on the services or an instance of cloud and forget to turn it off during the weekend or when there is no current use of it, it will increase the cost without even using the resources.

### 3. Multi-Cloud Environments

Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team. The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.

### 4. Performance Challenges

Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits. Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience. Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

### 5. Interoperability and Flexibility

 When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since applications written for one cloud with the application stack are required to be re-written for the other cloud. There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues encountered when changing cloud solutions, thereby reducing flexibility.

### 6. High Dependence on Network

Since cloud computing deals with provisioning resources in real-time, it deals with enormous amounts of data transfer to and from the servers. This is only made possible due to the availability of the high-speed network. Although these data and resources are exchanged over the network, this can prove to be highly vulnerable in case of limited bandwidth or cases when there is a sudden outage. Even when the enterprises can cut their hardware costs, they need to ensure that the internet bandwidth is high as well there are zero network outages, or else it can result in a potential business loss. It is therefore a major challenge for smaller enterprises that have to maintain network bandwidth that comes with a high cost.

### 7. Lack of Knowledge and Expertise

Due to the complex nature and the high demand for research working with the cloud often ends up being a highly tedious task. It requires immense knowledge and wide expertise on the subject. Although there are a lot of professionals in the field they need to constantly update themselves. Cloud computing is a highly paid job due to the extensive gap between demand and supply. There are a lot of vacancies but very few talented cloud engineers, developers, and professionals. Therefore, there is a need for upskilling so these professionals can actively understand, manage and develop cloud-based applications with minimum issues and maximum reliability.

**6 ORGANIZATIONAL CHALLENGES FOR CLOUD SERVICES**

**1. SECURITY**

Unlike an organization’s on-prem infrastructure, cloud-based deployments are outside of the physical network perimeter and can be directly accessible via the public internet. Without the right expertise and configuration, this can make it easier for **cybercriminals** to gain unauthorized access to cloud-based business solutions.

Cloud service providers offer a number of application programming interfaces (APIs) so that customers can get the most out of their cloud investments. If these cloud services are not carefully configured, crafty cybercriminals can exploit these APIs to gain unauthorized access. Gartner estimates that by **2022**, API abuses will be the single largest threat vector responsible for data breaches within enterprise web applications.

Cloud services often allow easy sharing of data. So great care should be taken with how things are set up to avoid sharing data with people who shouldn’t have access to that data. Insider threats are also a concern as malicious insiders can potentially provide access to someone not authorized.

**2. LACK OF EXPERTISE**

Studies suggest that **86%** of organizations are finding it challenging to find employees with the right skill-sets to configure and manage their cloud solutions, which is slowing down cloud projects. Cloud infrastructure is evolving so rapidly with an ever-increasing list of features, capabilities and changes that if employees aren’t keeping up with the latest trends and updates, it can cause massive security issues. Cloud misconfiguration is the number one reason for cloud data breaches world-wide and is also a major compliance risk.

**3. COMPLIANCE**

When businesses hand over data to a cloud provider, they don’t hand over the legal liability or the responsibility for regulatory compliance; that task stays with the company. On the flip side, IT doesn’t always have full control over provision, infrastructure delivery and operation in the cloud-based world; this can raise issues with compliance governance, data quality, and risk management.

Regulations are also tightening their grip on cloud services at the same time as originations are increasingly relying on them. Not only that, regulations are constantly changing and becoming more complex. Every country can potentially have a different regulation and this could lead to several gaps in compliance, especially for those businesses that are handling global customer data or Personally Identifiable Information (PII).

**4. COST**

Handling cloud spending is as difficult an issue to deal with as security. Those companies that try to ‘lift and shift’ their environment to the cloud are unlikely to find it cheaper than their on-prem environment. To extract real value from the cloud, companies need to undergo **digital transformation** by reimagining their functions, applications and services, instead of simply lifting and shifting their datacenter to the cloud.

Organizations are also finding it difficult to cope with the growing creep of cloud spending. Per recent research, almost **one-third** of cloud spending is getting wasted. As outlined earlier, there is a **major drought** of cloud talent and this means that finding, hiring and retaining the right person can be time consuming and expensive.

**5. MULTI-CLOUD**

Almost **93%** of companies use multi-cloud environments. This brings up a different set of complications because every cloud has a different mechanism, interface, and complexity. Multi-cloud can be expensive to manage and this may require a lot of different staff with different skills and capabilities. This also expands the threat surface drastically as the number of entry points such as third-party apps and APIs multiply (and because security teams are limited), monitoring the entire infrastructure can be difficult, thereby increasing the chances of security oversight and misconfigurations.

**6. CLOUD INTEGRATION AND MANAGEABILITY**

Most businesses use a combination of on-prem and multi-cloud environments (e.g., security, apps, tools, directory services, etc.). This can be difficult to integrate and manage since every environment will have a different way of monitoring performance. Without the right kind of tools and expertise put together in a centralized control panel, you may find that you don’t have proper visibility and control over how the network, applications and overall environment is performing. And even if you do have visibility, you’ve got it in different control panes of your various cloud providers. This results in organizations having to log into each of their cloud provider’s environments to see how each environment is performing – slowing down the discovery of potential issues.

Despite these challenges, if the cloud is well-implemented and managed, such issues are far from being showstoppers. There are technologies that can help too, such as **Citrix cloud services** that possess the ability to link into multiple environments and provide a single pane of glass for some aspects of user experience. Tools that can make your workspace intelligent can dramatically simplify accessibility and boost experience for users by providing access to the features rather than the entire app with all the different interfaces and settings.

# service-level agreement (SLA)

* A service-level agreement (SLA) is a contract between a service provider and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet.
* SLA stands for Service Level Agreement, it’s nothing but the service agreement between the service providers and the end users (clients) who are expecting the service from service providers in a given time frame. In this service agreement, it includes legal agreement because they involve money and other formal and informal contracts between internal & external business units.
* A service-level commitment (SLC) is a broader and more generalized form of an SLA. The two differ because an SLA is bidirectional and involves two teams. In contrast, an SLC is a single-directional obligation that establishes what a team can guarantee its customers at any given time.

## **Different Sections in SLA Includes**

* Whereby the service works
* Responsibilities of the Service
* Warranty of the Service
* Guarantee of the Service
* Ease and Performance of the Service
* Customer Support

Why we Need SLA

**Three reasons you should have an SLA with their service provider.**

**Establishing clear and measurable guidelines:**A Service Level Agreement (SLA) is vital to ensuring that client and service provider are on the same page in terms of service and standards. The agreement reduces the obligations between the client and service provider by setting clear and measurable guidelines.

**Unmet obligations are accountable:**If the service provider fails to meet their obligations they should pay for the reputation for the consequences occurred. In your SLA, you should include consequences if service provider performance is not met for standards. That’s why the service provider should always keep their goodwill with their client.

**A Client gets tension free with SLA:**The contract provides detailed information and provider accountability to the client. If any hurdles happen that goes with provider responsibility, so the client has a peacefulness at the end.

**Key components of an SLA**

Key components of a service-level agreement include:

**Agreement overview.** This first section sets forth the basics of the agreement, including the parties involved, the start date and a general introduction of the services provided.

**Description of services.** The SLA needs detailed descriptions of every service offered, under all possible circumstances, with the turnaround times included. Service definitions should include how the services are delivered, whether maintenance service is offered, what the hours of operation are, where dependencies exist, an outline of the processes and a list of all technology and applications used.

**Exclusions.** Specific services that are not offered should also be clearly defined to avoid confusion and eliminate room for assumptions from other parties.

**Service performance.** Performance measurement metrics and performance levels are defined. The client and service provider should agree on a list of all the metrics they will use to measure the service levels of the provider.

**Redressing.**Compensation or payment should be defined if a provider cannot properly fulfill their SLA.

**Stakeholders.** Clearly defines the parties involved in the agreement and establishes their responsibilities.

**Security.** All security measures that will be taken by the service provider are defined. Typically, this includes the drafting and consensus on antipoaching, IT security and nondisclosure agreements.

**Risk management and disaster recovery.** Risk management processes and a disaster recovery plan are established and clearly communicated.

**Service tracking and reporting.** This section defines the reporting structure, tracking intervals and stakeholders involved in the agreement.

**Periodic review and change processes.**The SLA and all established key performance indicators (KPIs) should be regularly reviewed. This process is defined as well as the appropriate process for making changes.

**Termination process.**The SLA should define the circumstances under which the agreement can be terminated or will expire. The notice period from either side should also be established.

**Signatures.**Finally, all stakeholders and authorized participants from both parties must sign the document to show their approval of every detail and process.

The Main Objectives of SLA

* Documentation
* Agreement
* Monitoring
* Measurement
* Reporting
* Reviewing
* Ensure to maintain good relationship & communication with customer (client)
* Ensure that businesses should understand the level of the service committed
* Ensure that appropriate measurements are taken to provide quality service

Different Types of SLA

They are three types of Service Level Agreements, depending upon the services requested by the client that will be provided to the customers (clients). The agreement is usually signed during the design stage itself.

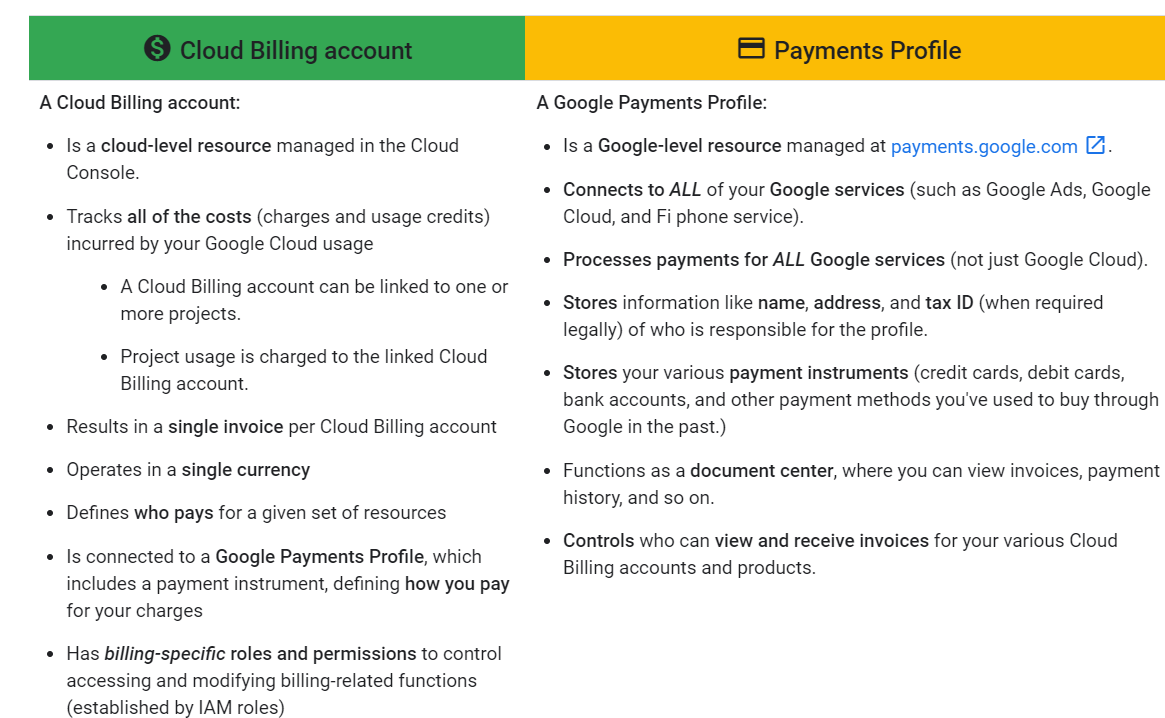
**1. Service Level SLA:**The service level SLA is also called service based SLA, an agreement that is same for all the customers who are using the services provided by the service provider. For e.g. if telecom network providing services and it charges for annual maintenance cost. The charges are same for all customers who are using the same **telecom network**.

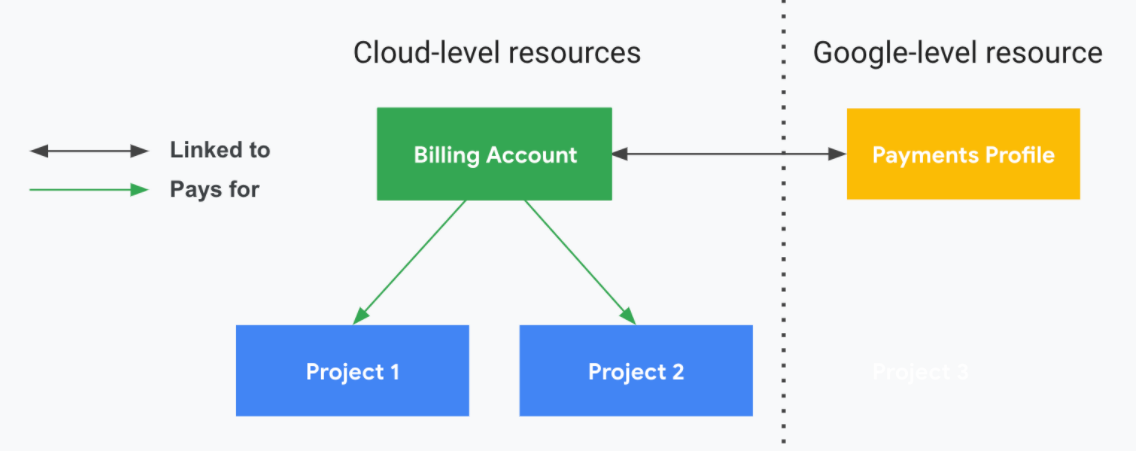
**2. Customer-Based SLA:**Second type of SLA is customer based SLA, an agreement that covers all the services used by this customer. For e.g. IT service provider provides different services like networking, maintenance, installations, monitoring and more to the customers and businesses and all are documented in one service level agreement, then it is called customer-based SLA.

**3. Multi-Level SLA:**The Multi-level SLA is again divided into three levels, each defining a different set of customers for the same services and different services for the specific set of customers. Maintaining SLA’s are part of service level management (SLM)

Cloud Billing and Accounting

* A Cloud Billing account is set up in Google Cloud and is used to define who pays for a given set of Google Cloud resources and Google Maps Platform APIs.
* Access control to a Cloud Billing account is established by IAM roles. A Cloud Billing account is connected to a Google payments profile. Your Google payments profile includes a payment instrument to which costs are charged.





Cloud Billing account types

* There are two types of Cloud Billing accounts:
* Self-serve (or Online) account
  + Payment instrument is a credit or debit card or ACH direct debit, depending on availability in each country or region.
  + Costs are charged automatically to the payment instrument connected to Cloud Billing account.
  + You can sign up for self-serve accounts online.
  + The documents generated for self-serve accounts include statements, payment receipts, and tax invoices, and are accessible in the Cloud Console.
* Invoiced (or Offline) account
  + Payment instrument can be check or wire transfer.
  + Invoices are sent by mail or electronically.
  + Invoices are also accessible in the Cloud Console, as are payment receipts.
  + You must be eligible for invoiced billing. Learn more about invoiced billing eligibility.

Payments profile types

* When you create your payments profile, you'll be asked to specify the profile type. This information must be accurate for tax and identity verification.
* This setting can't be changed. When you are setting up your payments profile, make sure to choose the type that best fits how you plan to use your profile.

There are two types of payments profiles:

1. Individual
   * You're using your account for your own personal payments.
   * If you register your payments profile as an individual, then only you can manage the profile. You won't be able to add or remove users, or change permissions on the profile.
2. Business

You're paying on behalf of a business, organization, partnership, or educational institution.You use Google payments center to pay for Play apps and games, and Google services like Google Ads, Google Cloud, and Fi phone service.

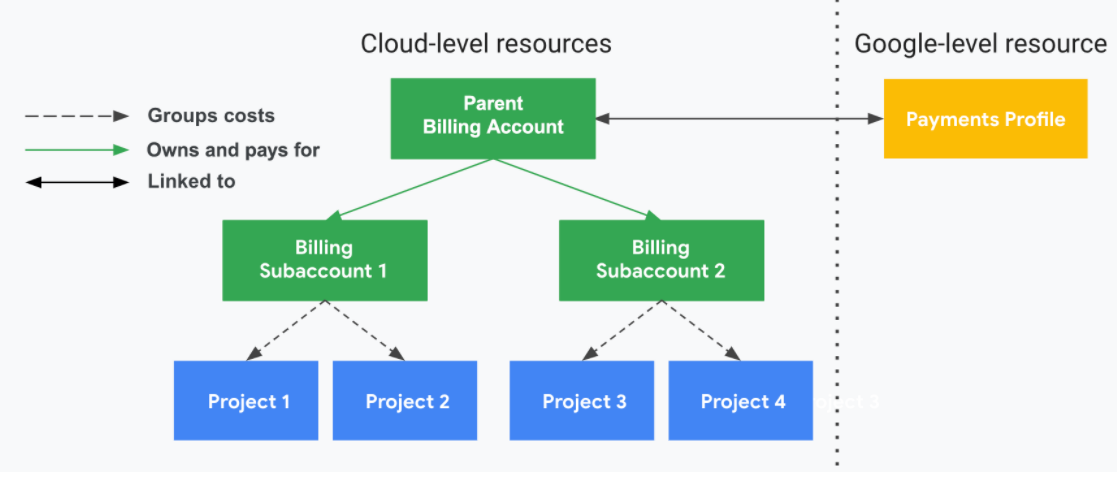
A business profile allows you to add other users to the Google payments profile you manage, so that more than one person can access or manage a payments profile.All users added to a business profile can see the payment information on that profile.

Charging cycle

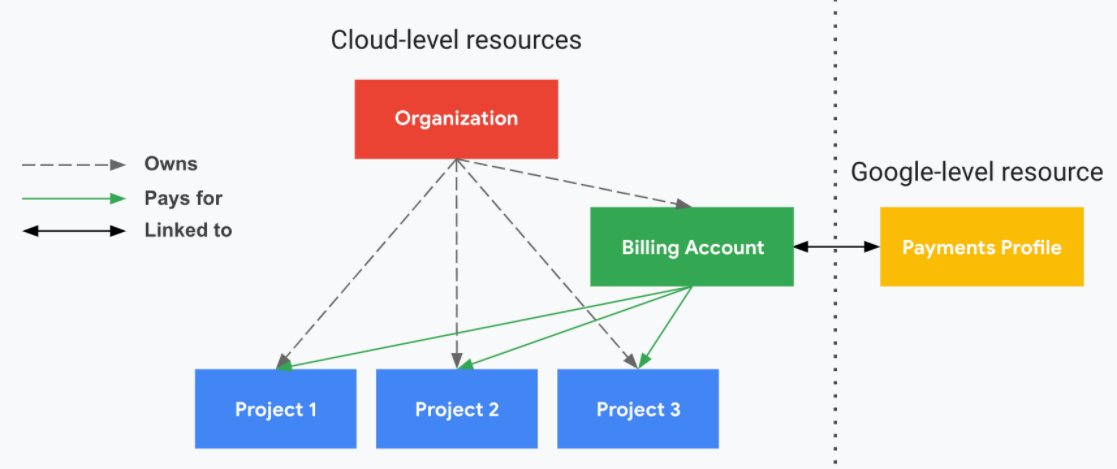
* The charging cycle on your Cloud Billing account determines how and when you pay for your Google Cloud services and your use of Google Maps Platform APIs.
* For self-serve Cloud Billing accounts, your Google Cloud costs are charged automatically in one of two ways:
* Monthly billing: Costs are charged on a regular monthly cycle.
* Threshold billing: Costs are charged when your account has accrued a specific amount.
* For self-serve Cloud Billing accounts, your charging cycle is automatically assigned when you create the account. You do not get to choose your charging cycle and you cannot change the charging cycle.
* For invoiced Cloud Billing accounts, you typically receive one invoice per month and the amount of time you have to pay your invoice (your payment terms) is determined by the agreement you made with Google.
* Billing contacts
  + A Cloud Billing account includes one or more contacts that are defined on the Google Payments profile that is connected to the Cloud Billing account.
  + These contacts are people who are designated to receive billing information specific to the payment instrument on file (for example, when a credit card needs to be updated).
  + To access and manage this list of contacts, you can use the Payments console or you can use the Cloud Console.

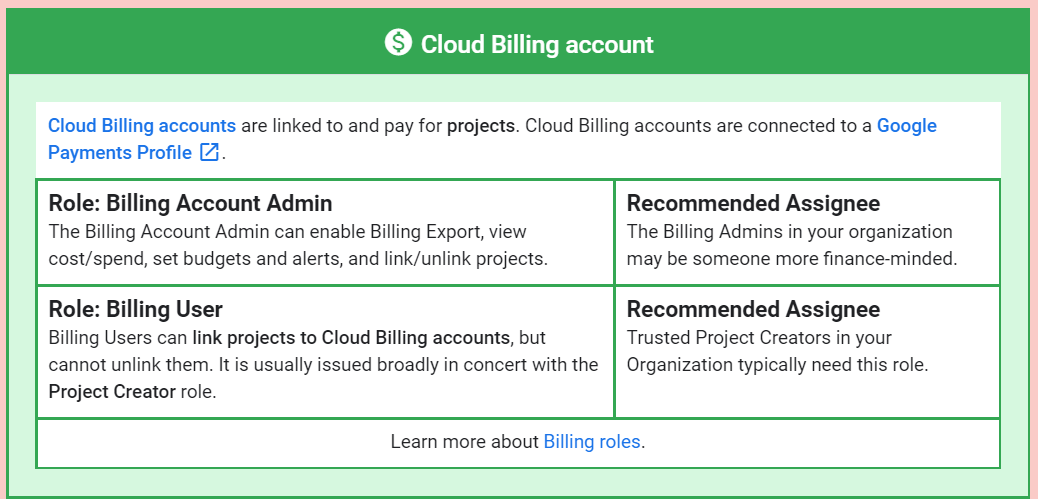
Subaccounts

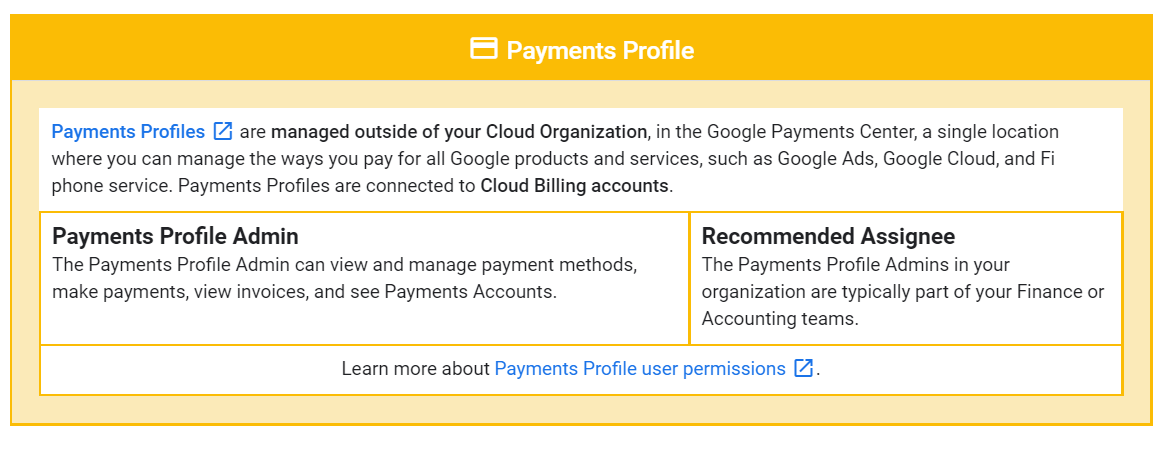
* + Subaccounts are intended for resellers.
  + If you are a reseller, you can use subaccounts to represent your customers' charges for the purpose of chargebacks.
* A subaccount behaves like a Cloud Billing account in most ways: it can have projects linked to it, Cloud Billing data exports can be configured on it, and it can have Identity and access management(IAM) roles defined on it.
* Any charges made to projects linked to the subaccount are grouped and subtotalled on the invoice, and the effect on resource management is that access control policy can be entirely segregated on the subaccount to allow for customer separation and management.



The following diagram shows the relationship of ownership and payment linkages for a sample organization.





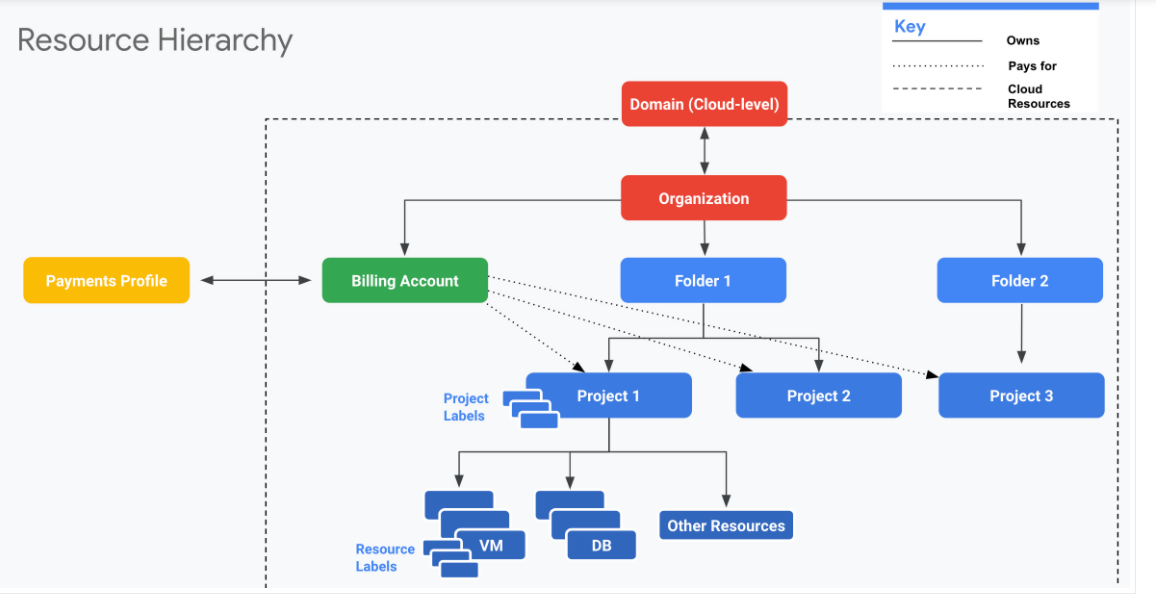


Managing Cloud Resources

* Resource management is focused on how you should configure and grant access to the various cloud resources for your company/team, specifically the setup and organization of the account-level resources that sit above the service-level resources.
* Account-level resources are the resources involved in setting up and administering your Google Cloud account.

Resource Hierarchy

* Google Cloud resources are organized hierarchically.
* This hierarchy allows you to map your organization's operational structure to Google Cloud, and to manage access control and permissions for groups of related resources.
* The resource hierarchy provides logical attach points for access management policies (Identity and Access Management) and Organization policies.



* Domain
  + - Your company Domain is the primary identity of your organization and establishes your company's identity with Google services, including Google Cloud.
    - You use the domain to manage the users in your organization.
    - At the domain level, you define which users should be associated with your organization when using Google Cloud.
    - Domain is also where you can universally administer policy for your users and devices (for example, enable 2-factor authentication, reset passwords for any users in your organization).
    - The Domain is linked to either a Google Workspace or Cloud Identity account.
    - The Google Workspace or Cloud Identity account is associated with exactly one Organization.
    - You manage the domain-level functionality using the Google Admin Console (admin.google.com).
* Organization
  + An Organization is the root node of the Google Cloud hierarchy of resources.
  + All Google Cloud resources that belong to an Organization are grouped under the Organization node, allowing you to define settings, permissions, and policies for all projects, folders, resources, and Cloud Billing accounts it parents.
  + An Organization is associated with exactly one Domain (established with either a Google Workspace or Cloud Identity account), and is created automatically when you set up your domain in Google Cloud.
  + Using an Organization, you can centrally manage your Google Cloud resources and your users' access to those resources. This includes:
    - Proactive management: reorganize resources as needed (for example, restructuring or spinning up a new division may require new projects and folders).
    - Reactive management: an Organization resource provides a safety net to regain access to lost resources (for example, if one of your team members loses their access or leaves the company).
* Folders
  + Folders are a grouping mechanism and can contain projects, other folders, or a combination of both.
  + To use folders, you must have an Organization node.
  + Folders and projects are all mapped under the Organization node.
  + Folders can be used to group resources that share common IAM policies.
  + While a folder can contain multiple folders or resources, a given folder or resource can have exactly one parent.
* Projects
  + Projects are required to use service-level resources (such as Compute Engine virtual machines (VMs), Pub/Sub topics, Cloud Storage buckets, and so on).
  + All service-level resources are parented by projects, the base-level organizing entity in Google Cloud.
  + You can use projects to represent logical projects, teams, environments, or other collections that map to a business function or structure.
  + Projects form the basis for enabling services, APIs, and IAM permissions.
  + Any given resource can only exist in one project.
* Resources
  + Google Cloud service-level resources are the fundamental components that make up all Google Cloud services, such as Compute Engine virtual machines (VMs), Pub/Sub topics, Cloud Storage buckets, and so on.
  + For billing and access control purposes, resources exist at the lowest level of a hierarchy that also includes projects and an organization.
* Labels
  + Labels help you categorize your Google Cloud resources (such as Compute Engine instances).
  + A label is a key-value pair.
  + You can attach labels to each resource, then filter the resources based on their labels.
  + Labels are great for cost tracking at a granular-level. Information about labels is forwarded to the billing system, so you can analyze your charges by label.