**What Is a Cloud Deployment Model?**

A cloud deployment model essentially defines where the infrastructure for your deployment resides and determines who has ownership and control over that infrastructure. It also determines the cloud’s nature and purpose.

The first port of call for any organization looking to adopt cloud services is to understand the available deployment models. Once these are understood, a better decision can be made about which routes the business should pursue. Each model will offer advantages and disadvantages in areas such as governance, scalability, security, flexibility, cost, and management.

**Types of Cloud Deployment Models**

Cloud deployment models can be divided into five main types

* [**Public Cloud**](https://spacelift.io/blog/cloud-deployment-models#public-cloud-model)
* [**Private Cloud**](https://spacelift.io/blog/cloud-deployment-models#private-cloud-model)
* [**Hybrid Cloud**](https://spacelift.io/blog/cloud-deployment-models#hybrid-cloud-model)
* [**Multi-Cloud**](https://spacelift.io/blog/cloud-deployment-models#multicloud-model)
* [**Community cloud**](https://spacelift.io/blog/cloud-deployment-models#community-cloud-model)

Let’s take a look at each model in more detail.

**Public Cloud Model**

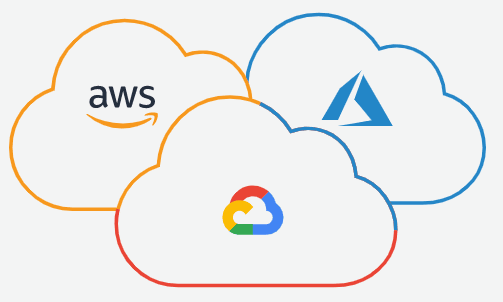
Public cloud is a commonly adopted cloud model, where **the cloud services provider owns the infrastructure and openly provides access to it for the public to consume**.

As the service provider owns the hardware and supporting networking infrastructure, it is under the service provider’s full control. The service provider is responsible for the physical security, maintenance, and management of the data center where the infrastructure resides. The underlying infrastructure is, therefore, outside of the customer’s control and also away from the customer’s physical location.

The cloud service provider will **share infrastructure between multiple customers whilst keeping data separate and isolated**, offering many layers of security controls where this is a concern. Some services can be hosted on dedicated or isolated hardware if required, usually at an additional cost. Cloud providers go to huge lengths to ensure physical data centers are extremely secure and are highly regulated environments, almost always exceeding the standards a customer could achieve themselves.

Infrastructure is managed primarily using a web browser but can also be manipulated using an API, on the command line, or using infrastructure-as-code tools such as Terraform.

Commonly used public clouds include Microsoft Azure, Amazon AWS, Google Cloud, Oracle Cloud, and Alibaba Cloud.



**Advantages of the Public Cloud Model**

* Low initial capital cost (Move from Capex to Opex)
* High Flexibility
* High (almost unlimited) scalability
* High Reliability
* Low maintenance costs

**Disadvantages of the Public Cloud Model**

* Data security concerns for strictly regulated businesses

**Private Cloud Model**

A private cloud can be thought of as **an environment that is fully owned and managed by a single tenant**. This option is usually chosen to alleviate any data security concerns that might exist with the public cloud offering. Any strict governance requirements can also be more easily adhered to, and the private cloud can be more easily customized.

Full control of the hardware can lead to higher performance. A customer will typically run a private cloud within their own building (on-premises) or purchase rackspace in a data center in which to host their infrastructure.

However, the responsibility to manage the infrastructure also falls to the customer, creating a need for more staff with wider skills and increasing costs. A large initial investment may also be required to purchase the required hardware.

**Advantages of the Private Cloud Model**

* Increased security and control
* Dedicated hardware may improve performance
* High flexibility

**Disadvantages of the Private Cloud Model**

* High cost
* Higher management overhead

**Hybrid Cloud Model**

The hybrid model **combines both public and private cloud deployment models** giving a single cloud infrastructure that is aimed at increasing flexibility and deployment options for the business.

For example, applications with strict governance and data security requirements may be hosted in the business private cloud, whereas applications without these concerns, which need to be scaled on demand, could be hosted in the public cloud.

The benefits of both the public and private cloud can be realized, as well as some of the disadvantages, such as increased management overhead and the initial challenge of setting up a hybrid infrastructure. Once realized, applications can be moved between infrastructure hosted in the public and private clouds, increasing flexibility and fault tolerance.

Typically businesses may have some presence on-premise, and utilizing this hardware until it has reached end-of-life in the private cloud will likely be an attractive option if the business already owns the hardware. In the hybrid model, this can be used to form part of the private cloud. Most businesses strive to alleviate the burden on the existing infrastructure, migrating to the public cloud where possible, and effectively utilizing the hybrid deployment model during the migration period.

**Advantages of the Hybrid Cloud**

* Improved scalability
* High control
* Highly scalable
* High fault tolerance
* Cost-effective

**Disadvantages of the Hybrid Cloud**

* Setup challenges
* High management overhead

**Multi-Cloud Model**

The multi-cloud deployment model usually refers to **the** **use of multiple public cloud providers to increase flexibility and fault tolerance**, such as the use of Microsoft Azure, Amazon AWS, and Google Cloud. The private cloud can also be thrown into the mix to give extra reliability and flexibility.

Some services may be preferred on a certain cloud over another after evaluation by the business. For example, the GKE (Google Kubernetes Engine) hosted on the Google Cloud may be preferable over similar offerings on Azure, such as AKS (Azure Kubernetes Service) or Amazon EKS (Elastic Kubernetes Service). Workloads can be distributed selectively.

Adopting multiple clouds gives development teams a choice from a much wider pool of options and can actually aid the developer workflow. Some comparable services may be cheaper than others and so may also be preferable in certain scenarios. For example, AWS could be used for production, and Google Cloud used for testing.

Multi-cloud is also commonly used by businesses with critical workloads, such as government agencies or financial corporations. Spreading data and infrastructure between multiple cloud providers can increase fault tolerance should one cloud platform encounter service outages. The benefits of the multi-cloud model can also be leveraged when a business forms a disaster recovery and business continuity plan.

However, with each option that is introduced, management becomes more complex, and staff requires more skills to fully realize the benefits of a multi-cloud deployment model. Depending on the business objectives, multi-cloud has the potential to lower costs or raise them if increased fault tolerance is the goal.

As with anything in I.T., the trade-off between the application requirements and the budget should be weighed up. Larger businesses further along the road in their cloud journey are usually suited to the multi-cloud model, as typically, a business will adopt and single public cloud and adopt another public cloud when the business requirements can be justified.

**Advantages of the Multi-Cloud Model**

* Very high reliability
* Very high flexibility

**Disadvantages of the Multi-Cloud Model**

* Increased management complexity
* Increased staffing skills required

**Community Cloud Model**

A lesser-known and less-adopted deployment model, a Community cloud brings together infrastructure that is **shared and jointly accessed by several organizations** **from a specific group** that shares specific computing needs.

For example, the education sector could utilize a community cloud to enable a group of scholars and students to share academic content, making joint research easier.

**Advantages of the Community Cloud Model**

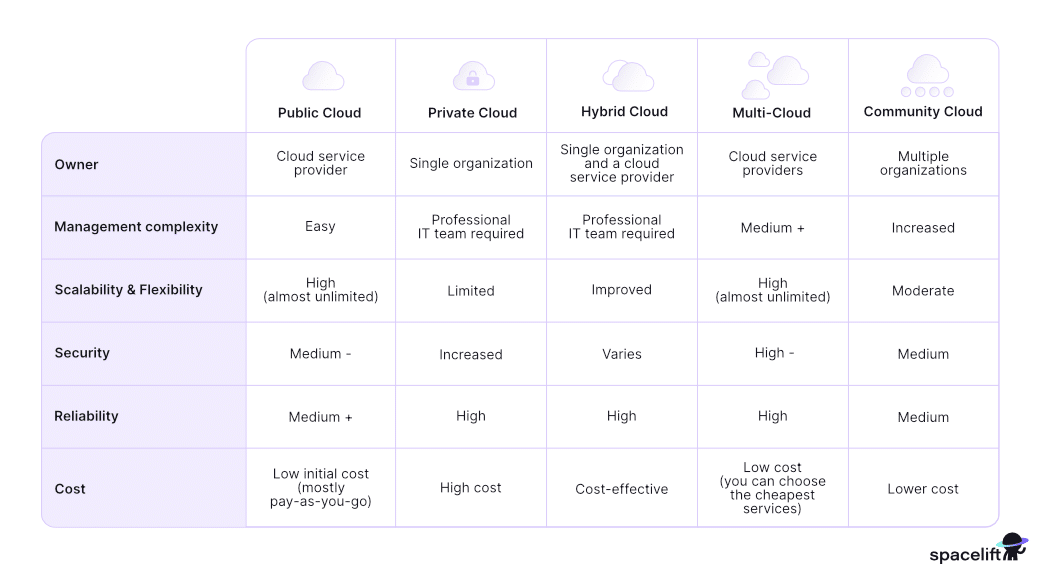
* Sharing infrastructure lowers costs

**Disadvantages of the Community Cloud Model**

* Reduced security
* Not applicable to most SMEs (Small to Medium enterprises)

**Cloud Deployment Models Comparison**

Below you can see the comparison table of previously mentioned cloud deployment models so you can make an informed decision when it comes time to take advantage of this modern infrastructure offering.



**Disadvantages of cloud computing infrastructure to on premises.**

Cloud computing benefits come with potential challenges, including the following:

* **Reliability.** Handing over control to a cloud provider also means relinquishing control over reliability. Cloud providers boast impressive uptime, but services occasionally go down. Even brief interruptions to cloud services can cause major problems for customers -- and there isn't much they can do but wait.
* **Complexity.** Cloud providers frequently expand their service portfolios. The more advanced a company's needs, the more complex it can be to select, implement and manage the appropriate cloud services.
* **Efficiency.** Application infrastructure that isn't designed for the cloud might not perform optimally. Internet connectivity and speed, permissions management and other factors can potentially reduce application efficiency.
* **Less flexibility.** Cloud-based software often comes as off-the-shelf, one-size-fits-all applications and, therefore, lacks flexibility and customizability.
* **Vendor lock-in.** The more a company uses cloud-based infrastructure from one provider, the greater the risk of vendor lock-in. It may be difficult to migrate to a different provider's infrastructure -- or even move back on premises.
* **Cost management.** If organizations aren't careful, they might inadvertently use more cloud services than planned. Huge upticks in resource requirements can quickly break the bank. Long-term subscription costs for cloud-based software can add up and may eventually exceed the cost of an upfront software licensing fee.
* **Storage costs.**The costs for housing applications in the cloud grow slowly and can accumulate unnoticed if not allocated and monitored properly. Plus, unused data residing in the cloud can bloat the monthly cloud storage bill.
* **Specialized skills.** Some traditional systems administrator skills may be less applicable in the cloud, and engineers need to master other cloud skill sets -- from utilizing identity and access management (IAM) to understanding the nuances behind countless services on the platform.
* **Security.** Migration and operation in the cloud come with inherent security risks. Though cloud security has improved, organizations need to ensure that cloud-based software packages support embedded security measures, like single sign-on and multifactor authentication.