Choosing a Cloud Vendor: Benefits, Drawbacks and Considerations

venminder

Choosing a Cloud Vendor: Benefits, Drawbacks and Considerations

These days, most have heard of "the cloud." However, not everyone is sure what that means or what the cloud actually is. The term "cloud" refers to a wide range of services and applications. There's a good chance that your organization is already using cloud services or will use them soon, so it's worth learning some of the basics. This eBook will help you understand what the cloud is and how cloud services and applications are used. We'll also review some considerations for choosing and managing a cloud service provider.

Cloud Basics

Introduction to the Cloud

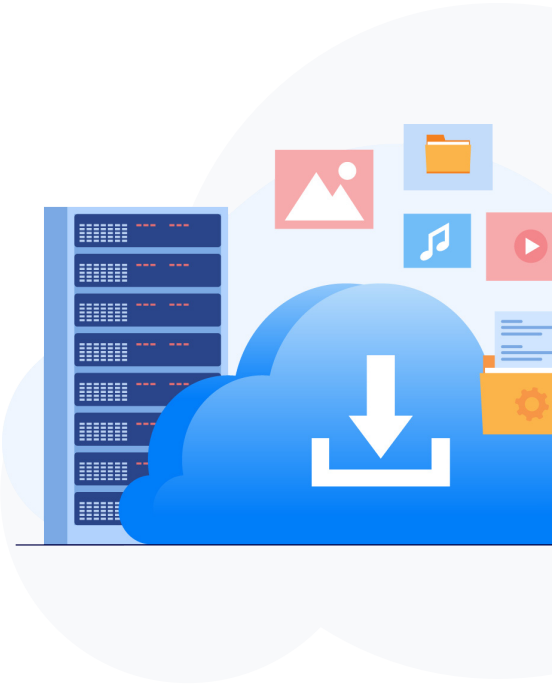
The term cloud tends to evoke images of ethereal data floating around in the air. While that is an interesting image, it isn't accurate. The term cloud comes from old telecom and network diagrams where the symbol of the cloud represented a somewhat abstract data location or network. Today, the term cloud refers to a network of remote systems which can be located anywhere. These systems are connected and meant to operate as a single ecosystem.

A popular saying goes, "the cloud is just another computer on somebody else's desk," however, that is an overly simplistic view. Cloud computing and storage are based on a distributed network of computers, servers, computing power, databases, applications and development delivered via the internet, rather than sitting on your desktop, network or data center. The cloud helps organizations gain economies of scale and flexibility because services can be scaled up or down depending on their needs. Also, cloud services and storage can sometimes be more cost-efficient because organizations are only paying for what they use. However, this isn't always the case, as the cost can vary depending on the organization's operational expenses. The cloud gives an organization the ability to essentially rent compute and data storage services rather than purchasing and maintaining all that technology and environmental infrastructure.

Cloud Storage and Services

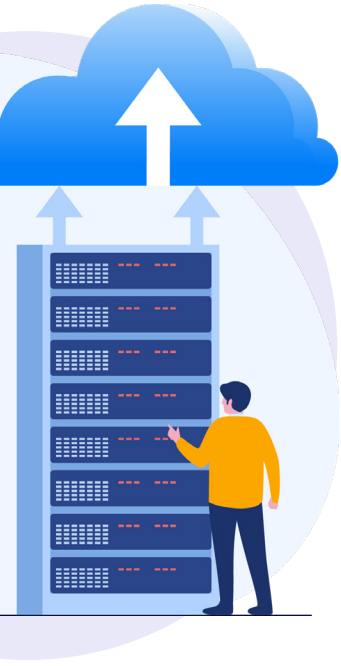
Cloud technology can often be used for data storage or services. Some of your vendors may utilize the cloud within their own operations or may have cloud subcontractors (your fourth parties). Regardless of whether your third or fourth parties are using this technology, it's important to know that not every cloud is the same and not all forms of cloud services or storage are suitable for every organization. Several different models, types and services are available and serve different purposes.

Depending on your organization, you may use one or more of the following options:



- **Cloud Storage**
  A cloud storage space is an internet-accessible space where data is stored on remote servers. Data is managed, maintained and backed up remotely and users pay a monthly or per-consumption fee. Cloud storage involves storing data in data centers on servers and making it available for users online. Users can upload their content remotely, store it and access it whenever necessary.

- **Cloud Services**



  - **Infrastructure as a Service (IaaS)**
    As a service, infrastructure as a service (IaaS) is the most basic type of cloud computing. A cloud provider offers you IaaS, which allows you to rent infrastructure, servers, virtual machines, storage, networks and operating systems on an as needed basis.

  - **Platform as a Service (PaaS)**
    A platform as a service is a cloud computing service that provides an on-demand environment for developing, testing, deploying and managing software applications. With PaaS, developers don't have to worry about setting up or managing servers, storage, networks or databases needed to build web or mobile apps.

  - **Software as a Service (SaaS)**
    This cloud service delivers software over the internet, typically via subscription. Connecting to the application is done through a web browser, usually on a smartphone, tablet or PC. SaaS providers are responsible for hosting and maintaining the software application and underlying infrastructure, and for any maintenance, such as software upgrades or security patches.

Cloud Deployment Models

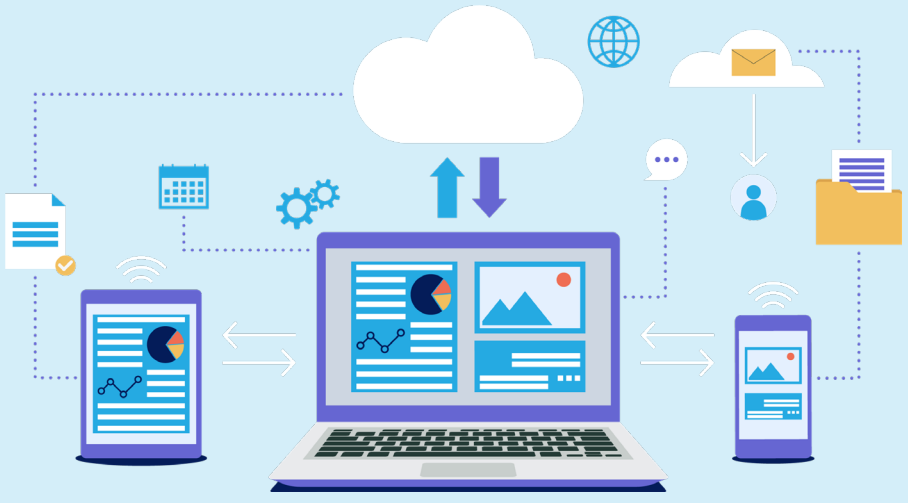
As with cloud services, there are many ways to implement and deploy the cloud. Deploying cloud services can be done via these three models:

- **Public Cloud**
  This model is owned and operated by third-party cloud service providers which deliver their computing resources, like servers and storage, over the internet. These services are accessed and managed through a web browser. The cloud provider is responsible for owning and managing all hardware, software and other infrastructure supporting the public cloud. Almost all major technology companies offer cloud services. Amazon Web Services (AWS), Microsoft Azure, Google Cloud and Salesforce are all examples of public providers.

- **Private Cloud**
  The private cloud is a cloud computing resource used exclusively by one company or organization. In a private cloud, services and infrastructure are maintained on a private network. Private clouds may be hosted in the company's own data center or by a third party.

- **Hybrid Cloud**
  In hybrid clouds, public clouds and private clouds are woven together via technology that makes it possible to share data and applications. As data and applications can be moved between private and public clouds, a hybrid cloud can improve an organization's flexibility, provide more deployment options and potentially optimize existing infrastructure and security.

- **Community Cloud**
  This model shares resources with a group of organizations or within an industry such as government or credit unions. Only members within those communities would be able to access the cloud.



Common Benefits & Drawbacks of the Cloud

There are undoubtedly many benefits of the cloud, but there are also some potential drawbacks. When you consider the third-party risk management lifecycle, it's important to understand any special factors when it comes to managing cloud vendors. As you perform an initial risk assessment of your vendors, it's important to identify the unique risks and challenges that cloud vendors can pose to your organization. Keep in mind that every organization has unique needs when it comes to using the cloud, and the benefits and drawbacks won't be identical for everyone. The environment that your organization is coming from and moving to will play a role in whether certain factors will be beneficial or unfavorable.

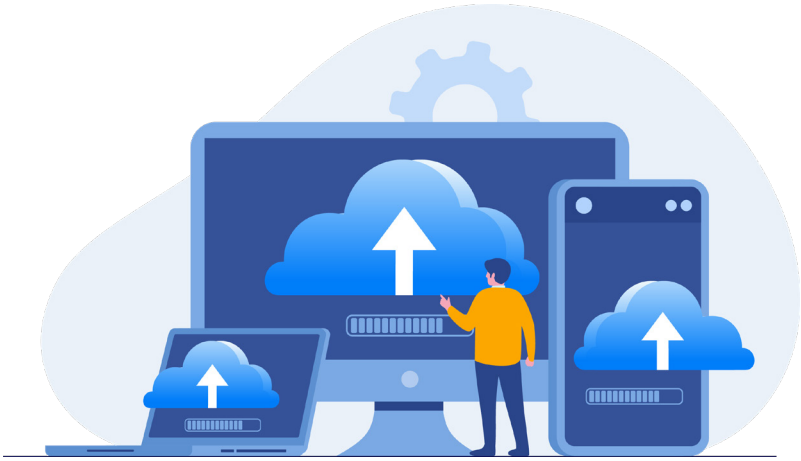
Let's consider some commonly seen advantages and disadvantages of the cloud:

ADVANTAGE	*DISADVANTAGE*
High Speed With cloud computing, you can put your service in place quickly and with fewer clicks. It allows you to get the resources you need for your system in less time.	**Limited Data Transfer** Cloud storage providers usually limit their customers' data transfer usage. As such, if your organization exceeds the given allowance, the additional charge could be quite costly.
Automated Software Integration Software integration takes place automatically in the cloud, so you don't have to spend additional time and resources on customizing and integrating your applications.	**Technical Issues** Outages and other technical difficulties are always a risk with cloud technology. Although cloud service providers maintain high standards of maintenance, they may still encounter this type of trouble.

ADVANTAGE	DISADVANTAGE
Ease of Data Backup and Restoration Data stored in the cloud makes backing it up and recovering it easier, something that is otherwise very time-consuming on premise.	**Cyber Threats** Working with cloud computing services has security risks, depending on how well it's protected. As a result of adopting cloud computing, you'll be sharing your organization's sensitive data with a third party. Hackers may exploit the data that you are sharing.
Mobility In the office or at remote locations, employees typically have easy access to all the services available, provided that the cloud is set up for this capability. All they need is access to the internet.	**Internet-Dependent** Cloud computing often requires a good internet connection. The cloud is generally inaccessible without it. Without internet access, you don't have any other way to gather data from the cloud.
Cost Savings Cloud computing sometimes offers cost savings as one of its biggest benefits. It can often save you a lot of money because it doesn't require any physical investments in hardware. Moreover, you don't need trained personnel to maintain the hardware. The cloud service provider is responsible for purchasing and managing the hardware.	**Lack of Support** Most cloud computing companies don't provide customers with adequate support. In addition, they want their users to rely on FAQs or other self-service resources, which can be challenging for non-technical people.

What to Consider When Choosing a Cloud Provider/Vendor

It's vital to assess the reliability and capability of a service provider that you plan to entrust with your organization's applications and data. Before choosing a new provider or re-assessing an existing provider, here are some important considerations.



Note: *Remember that the responsibilities of managing the cloud will shift between you and the provider, depending on the type of service provided. You should create a shared responsibility matrix for each of your cloud service providers to better understand where the responsibilities fall between each party.*

General Features

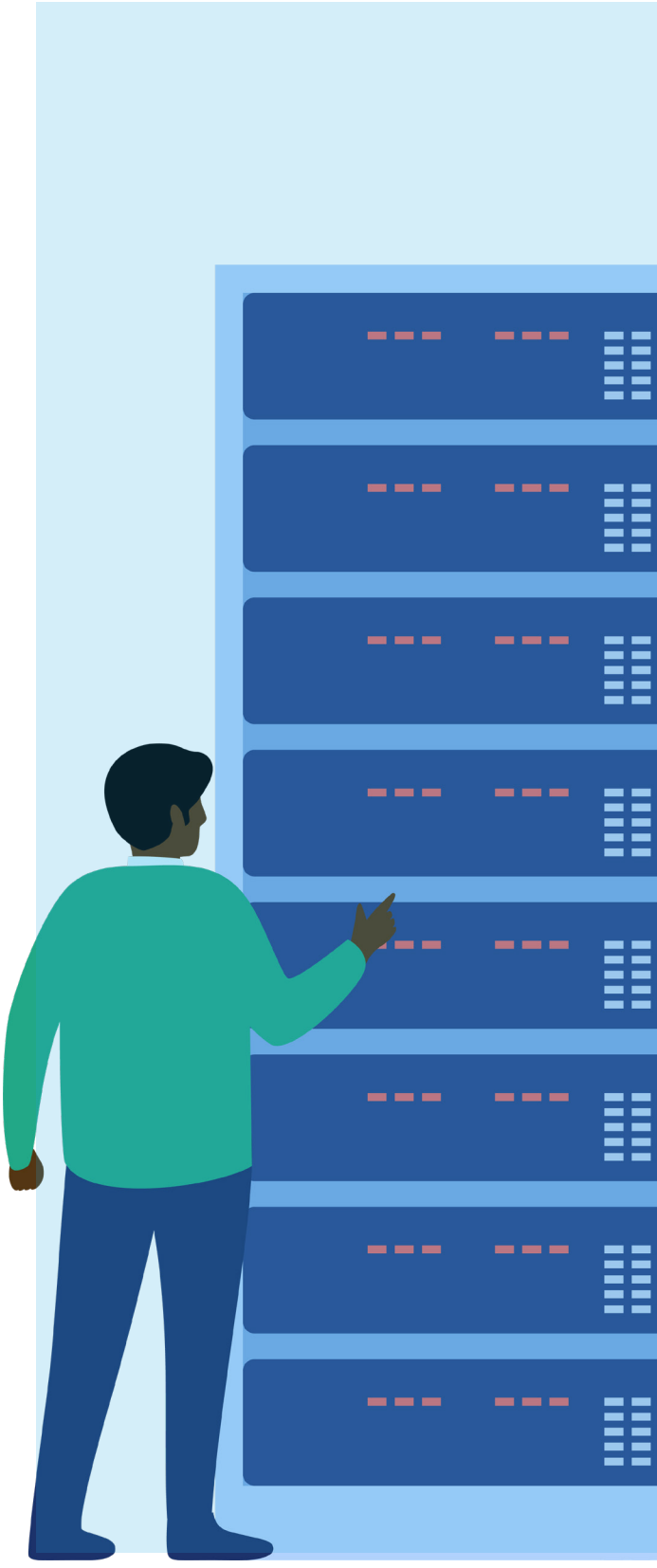
- **Technical expertise and business knowledge** – An experienced provider should know your business and be able to match your technical needs with their expertise.
- **Management of risk, organization and governance** – It's essential for a provider to have a formal management structure, established risk management policies and a formal evaluation process for third-party vendors and service providers.
- **Service level agreements (SLAs)** – You should be able to expect basic service level guarantees from your providers.
- **Billing and accounting** – Accounting should be automated so that you can monitor the cost and resources used so you avoid racking up unexpected bills. You should also know what support and resources are available for any billing issues that arise.
- **The ease of deployment, management and upgrades** – Make sure the provider offers easy-to-use deployment, management and upgrade mechanisms.
- **Standard interfaces** – Application programming interfaces (APIs) and data transformations should be standard so that your organization can easily build connections to the cloud.

Cloud Management and Administration

- **Change management** – A provider should have documented formal processes for requesting, logging, approving, testing and accepting changes.
- **Configuration management and resource monitoring** – Controls should be in place for the provider to monitor and track any changes to their systems as well as the services provided to customers.
- **Event management** – Ideally, the provider should have a formal system for managing events that are integrated with its monitoring and management system.

Security Practices

- **Security policies** – Providers should have comprehensive security policies in place for controlling network access to customers' and providers' systems.
- **Security infrastructure** – In order to provide comprehensive security of all types and levels of cloud services, it's imperative that appropriate security infrastructure is in place.
- **Identity management** – Any changes to an application service or hardware component should require personal or group authorization and authentication should be required for anyone making changes.
- **Backing up and retaining data** – In order for customer data to be protected, policies and procedures should be in place and operational.



- **Physical security** – Controls should be in place to ensure physical security, including controls for access to co-located hardware. A data center should also have environmental safeguards in place to protect equipment and data.

- **Ongoing monitoring** – Because cloud vendors can expose you to cyber threats, it's essential to establish a strong practice of ongoing monitoring. This will help ensure that any new or emerging risks are quickly identified and addressed.

Other Considerations

- **Business continuity and disaster recovery** – The provider should have a tested plan for business continuity and disaster recovery, including backup power and networking infrastructure.

- **Financial health** – In order to operate successfully over the long term, the service provider should have a track record of stability and be financially healthy.

- **Provider reputation** – Review the provider's reputation as well as its partners. Find out how experienced the provider is with cloud computing. Look up reviews and talk to customers when possible.

- **Regulatory and legal compliance** – A provider should have a compliance policy and conduct regular employee compliance training.

- **Third-party audits or certifications** – A provider should have tested controls through independent third-party audits.

- **Exit strategy** – Consider your exit strategy requirements when offboarding a cloud provider. This could include revoking vendor access to your systems, transitioning to a different cloud vendor or bringing the activity in-house.

The cloud offers organizations exciting and innovative ways to access, store, transmit and process data and applications of all types. In contrast to on-premise data storage and computing, using the cloud eliminates the need to invest in costly hardware, infrastructure and management, so many organizations often see it as an attractive option. Still, using the cloud is dependent on the internet, which can be rife with technological and security concerns. Ensure your organization can balance the risks and rewards of the cloud by identifying the potential risks and thoroughly vetting your cloud providers to make sure they meet your requirements.

Download free samples of control assessments and see how Venminder can help reduce your third-party risk management workload.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.