

# Ensuring Security in the Cloud

Over the last several years, cloud computing has emerged from a promising concept to one of the most demanded IT hosting solutions. With a devastating recession in full effect, more businesses are coming to realize that they can tap into the cloud to access state of the art applications and infrastructures at a fraction of the cost. While the benefits cannot be denied, the security risks are becoming more of a scary reality everyday. Here are a few tips to help make sure your investment in the cloud is secure.

## Access Control

The fact that you are trusting your sensitive business data to an outside party is a considerable security risks in itself. This is because relying on an outsourced service bypasses the physical, personal and logical controls employed for internal environments. For this reason, you want to gather all the information you possibly can to learn more about the parties that you will be handling your data. Ask the provider about privileged administrators and what level of access they will have to your data.

## Data Security

In the end, you are responsible for ensuring the security and integrity of your own data. This is the case even when it is in hands of a cloud computing service provider. With that said, most companies are subject to third-party audits and security certifications in order to meet regulatory compliance. This works in your favor but since nothing is guaranteed, it is up to you to find out what measures the provider is taking to protect your data before making any commitments.

## Learn About Location

When leveraging the cloud, there is a great possibility that you will have no idea of where your data is actually stored. Due to the prevalence of global cloud networks and infrastructures, you might not even know what country it is located in. If you are truly concerned about the protection of your data, you should seek out a provider that makes a commitment to storing and processing this information in certain jurisdictions while ensuring that all privacy policies are upheld.

## Dependable Encryption

In most cases, cloud data is stored in a shared environment, meaning it is residing beside information owned by other customers. While encryption is effective, it is not the cure-all solution to security. Therefore, you need to find out what is being done to protect data while it lies resting in the cloud. A reliable provider will only utilize encryption schemes that have been tried and tested by security experts. The use of a viable cryptography system is crucial because encryption flaws can make data completely inaccessible and result in excessive downtime.

## Backup and Recovery

Should you sign on for a cloud computing solution and you cannot find out where your data will be stored, the host should still be able to let you know the consequences in light of a disaster. However, if they are not backing up your data and applications on a regular basis, then you are more susceptible to losing everything you placed in the cloud. To ensure business continuity, make sure the firm has the ability to provide complete restoration in a timely manner.

## Seek Out a Long-Term Solution

In an ideal situation, your original cloud computing provider will never go out of business due to the lack of financial resources or being acquired by a larger firm. In the real world, you need to make sure that your data remains accessible even if such a scenario should be the case. Find

out how your data would be affected under these conditions and learn how it can be retrieved and imported into alternative cloud applications.

[Via WebHostingFan](#)