# CLOUD COMPLIANCE EXPLAINED: 4 KEYS FOR SUCCESS

Cloud compliance is a huge issue for a majority of organizations, and it all begins the second you decide to migrate your data to the cloud. Until recently, most Cloud Service Providers (CSPs) only focused on providing data storage and cloud storage services to companies, without much energy dedicated to the security of that data or whether it met industry regulations. As the cloud playing field is expanding, and becoming more competitive, CSPs are more aware of how to help customers achieve cloud compliance as well as the best way to follow new guidelines and compliance updates.

With national and industry regulations for how you store data in the cloud constantly changing and being updated, it may seem like an impossible task to maintain compliance. We have put together four keys for success to achieve compliance in the cloud.

## Be Aware of Regulations and Guidelines

One of the biggest aspects of cloud compliance involves a variety of industry standards and regulations of which anyone using the cloud must comply. Of these regulations, there are typically local, national, and even international standards that must be followed, all with specialized and technical language, giving even the most intelligent employee a headache.

CSPs, on the other hand, are now more equipped than ever to deal with these various guidelines, and most even have a dedicated team of experts that work continuously to ensure compliance. This is extremely beneficial for you as you get access to all of their compliance infrastructure right away, and let their teams handle the audits. Typically, you can even download all of the audit reports needed to demonstrate compliance.

The most important thing your company needs to do, then, is become aware of all of the regulatory policies and procedures you must comply with, and then find a CSP that meets the same set of standards. The CSP should be able to provide documentation of how they meet compliance in the cloud, and also be able to prove it in an audit.

Some of the most common regulatory requirements include HIPAA, PCI DSS, and GLBA.

HIPAA (Health Insurance Portability and Accountability Act) is a set of healthcare laws that lays out strict guidelines and security protocols for how patient health data and confidential information can be stored. These laws apply to healthcare providers, such as doctors and hospitals, as well as health insurance companies. The best way to meet compliance for HIPAA protocols is to securely encrypt data to protect it in the event of a security breach.

PCI DSS (Payment Card Industry Data Security Standard) is a standard that is required of any company that processes or handles payment card information, such as credit cards. Each of the 12 requirements must be met in order to achieve compliance, and a failure to do so can result in hefty fines.

The GLBA (Gramm-Leach-Bliley Act) law applies to financial institutions regarding how they protect the security of customers' confidential information. This law states that companies must explicitly share with customers how their data is being stored, as well as what measures are being followed to protect it.

## Access Control

Lack of proper authentication, or identity and access control, is a major source of company data breaches, but it does not have to be. Many companies begin seeing multi-factor authentication as too complex and time-consuming to dedicate energy for, however, this is one of the best ways to avoid potential security threats. While a single sign-on can be convenient for users, it greatly increases the risk of being hacked, and one username or password alone is extremely easy to steal, especially if employees use poor passwords.

The best way to alleviate the risk of being compromised is through multi-factor authentication. Multi-factor authentication is a highly secure process that makes it near impossible to be breached. In order to login, users must not only utilize a username and password, but they must also use a second source of authentication, such as a verification code sent to their phone or email. This reduces the ability for someone to login with usernames and passwords as there is another step needed that only the approved employee can finish.

## Classify Data and Know Where Data is Stored

One of the most important pieces of maintaining cloud compliance is knowing where your data is being stored. If you should ever undergo an audit, you will need to prove the exact location of your data as well as what you have put in place to protect it.

When you are researching potential CSPs, be sure to obtain explicit documentation from them about the location of their servers. According to a majority of industry standards and regulations, any server used by a CSP to store data should reside in the United States. Even if you find certain regulations that do not require the servers to be in the U.S., other countries many have different laws, which can then turn into a huge privacy issue.

Once you have decided on a reputable and legitimate CSP, the next step for your company is to classify all of your data to choose what will be moved to the cloud. For both compliance and security reasons, it is advised that highly confidential or sensitive data remains on the internal network and is never migrated to the cloud. Another option for companies it to use a private cloud that is hosted right on the premises, providing the benefits of cloud storage without all of the same security risks.

## Encrypt, Encrypt, Encrypt

After you have done a thorough classification of all of your data, and have decided that there is some confidential and sensitive information that must be stored on the cloud, then it is vital to make sure that your company encrypts the data. By encrypting your sensitive data, it not only further protects it from attacks or compromises, it also ensures that it meets most compliance requirements. A majority of CSP offer encryption services for you, but there are also many third-party software programs that can help you with the process.

If your CSP provides the encryption, you will need to find out what type of encryption they use as well as how and when it is applied. Although your CSP may offer these services, it is important to keep in mind that it is still your responsibility to protect the data, both while it is being moved and while it is being stored. During transit, there are industry standard transport protocols, like https, which alerts you that the communications between you and the server is encrypted.

What is most vital in this whole process, however, is how the data is stored. More than 60% of data breaches are carried out by insiders from the company, whether they are malicious or simply accidental, which means that those with direct access to your data could cause it harm. By encrypting all data between internal servers behind your firewall, it adds an extra layer of protection against employees trying to steal information, or those who inadvertently access confidential files.

CSP set up virtual networks that no one within your company has access to, and in which all traffic flowing between machines in the cloud is encrypted. This helps to eliminate the risk of data being intercepted or hacked into. As an organization, there are a few steps you can take to prevent insider threats:

- Identity management
- Identity governance
- Access management and risk-authentication
- Security intelligence

On a side note, HIPAA requirements state that all data stored on hard drives, whether internal or those of the CSP, must be encrypted. Any backup copies of the data must also be encrypted, and every hard drive must be accounted for at all times.

## Conclusion

Whether your organization is using a private cloud or a public cloud, there are many guidelines that must be met in order to ensure cloud compliance. A majority of cloud service providers have begun to recognize the importance of offering services to their customers to achieve compliance, and they are continually looking at their processes to improve. No matter what type of cloud you may end up choosing, the data that you migrate to it must meet all of the compliance regulations and guidelines.

## Resources from BMC

SecOps is the seamless collaboration between IT Security and IT Operations to effectively mitigate risk. BMC SecOps solutions enable your teams to prioritize and remediate critical vulnerabilities, and systematically address compliance violations through an integrated and automated approach across all environments.

BladeLogic Server Automation and BladeLogic Network Automation provide the full cycle of system discovery, monitoring, remediation, and integrated change control, providing continuous compliance with out-of-the-box integration with BMC Remedy Service Management Suite.

- Achieve compliance twice as fast with pre-configured policies for CIS, DISA, HIPAA, PCI, SOX, NIST, and SCAP.
- Simplify repair, rollback, and configuration updates with integrated documentation and remediation.
- Combine with BMC BMC Helix Discovery to discover all software, hardware, network, storage and versions within the data center and view the dependencies between all these assets.