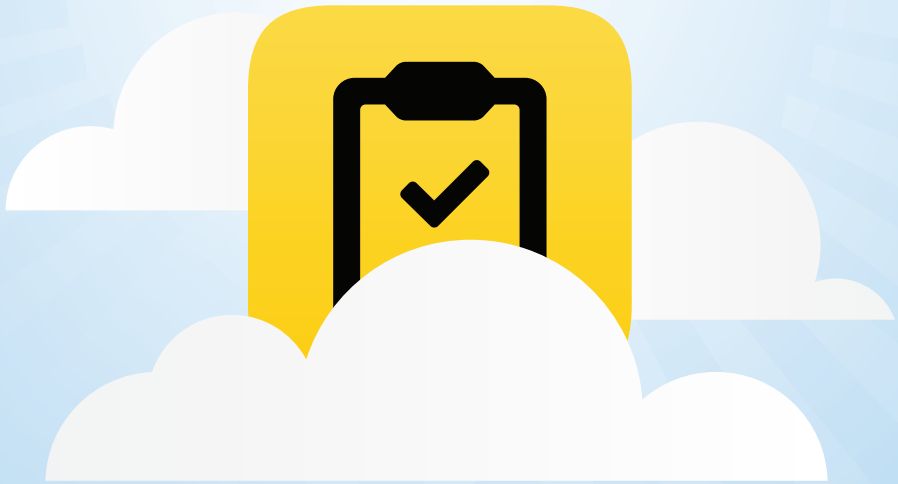
SPANNING by EMC

White Paper

Compliance in the Cloud: SaaS Data Backup and Restore Get the Job Done

JUNE 2014



If you operate any kind of organization today, chances are good that you're required to comply with at least one of the many laws regulating how organizations manage information and data.

Chances are also good that the regulations with which you must comply have to do specifically with information security, particularly as it concerns the confidentiality, integrity, and availability of data.

Compliance with these regulations may mean legal liability, whether the information affected by them is in an on-premises system or in the cloud. And data backup is an issue wherever the data resides, too. If you use SaaS applications like Google Apps or Salesforce, reducing the risk of losing mission-critical data you're storing in them is imperative to reducing your compliance risk.

Why Backup Is Critical for SaaS Applications

Of course, your cloud application provider should be taking steps to protect your data, and companies like Google and Salesforce have a number of security controls in place to help protect the data in their applications. But there's always a risk of data loss due to factors beyond these SaaS providers' control - things like sync errors, hacking, and human error. That's why backup is so important for SaaS applications. It's not always explicitly required, but it's critical to have in order to protect your business from both data loss, productivity loss, and non-compliance.

Often a regulation will only generally say that you must "keep information available" – and then leave it to you to determine what that means. The *Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley)*, for example, mandates that certain kinds of information be retained for five years. But if you're going to ensure that records are kept available for that period, it stands to reason that you need to have an effective backup solution in the event something happens to them.

Reducing the risk of losing data in SaaS apps is imperative to reducing compliance risk.

How Compliance Frameworks Can Help

If regulations don't always spell out the actions to take, how do you determine exactly how to comply with regulations? A number of compliance frameworks have emerged that include specific standards and controls to enable compliance. Meeting these standards and implementing these controls puts organizations on a path to meeting the broader requirements of regulations.

Focusing on those frameworks that include backup as a means of achieving compliance, we offer this information to help you become more familiar with:

- Backup-related regulatory expectations on your organizations for SaaS applications like Google Apps and Salesforce;
- Standards and controls that frameworks offer to meet those expectations; and,
- Characteristics to look for in cloud-to-cloud backup solutions.

MANDATE	DESCRIPTION
Cloud Security Alliance's Cloud Controls Matrix	While only one of these refers directly to backup and recovery, the other two suggest that an appropriate backup solution will address both recovery time objectives (RTOs) and the ability to make data available on request: • *Control ID BCR-12* calls for backup and recovery measures to be incorporated as part of business continuity planning and tested accordingly for effectiveness. • *Control ID GRM-12* speaks to establishing acceptable levels of risk in accordance with reasonable resolution time frames. • *Control ID IPY-02* requires that data be available to customers and provided to them on request in an industry-standard format. Download the Cloud Controls Matrix here.

MANDATE	DESCRIPTION
COBIT (Control Objectives for Information and Related Technology)	COBIT's emphasis on recovery points to the need for a backup and recovery solution that is reliable and easy to use, and that enables data to be recovered as quickly as possible to minimize disruption: • *Control Objective DS 11* states that a proper strategy for backup and restoration should be implemented, including developing and testing of a recovery plan. • *Control Objective DS 4* stresses the importance of minimizing the impact of any disruption on business operations and provides guidance for activities such as backup recovery.
NIST (National Institute of Standards and Technology) Recommended Security Controls	NIST's Recommended Security Controls pertain specifically to federal agencies and organizations that work with them. *CP-9 Information System Backup* requires "backups of user-level and system-level information (including system state information) contained in the information system." This language suggests that organizations should be backing up not only critical data, but also data customizations and metadata.
HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule	Healthcare data is among the most sensitive anywhere. The ability to protect that data is therefore critical. The HIPAA Privacy Rule *CFR 45 Part 164* directs organizations to "establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information," as well as to "establish (and implement as needed) procedures to restore any loss of data."
AICPA (American Institute of CPAs) SOCs (Service Organization Controls)	The AICPA SOCs constitute a framework of accounting standards and controls that auditors can apply to their work. SSAE 16 focuses on an organization's ability to maintain rigorous operational and security controls. Among the criteria for compliance are the existence of procedures to provide for data backup, offsite storage, and restoration.

What Happens When You Don't Comply – and When You Do

Consequences of non-compliance

- *Failed audits.* Addressing areas of concern identified in an auditor's report can take weeks or months and siphon off valuable internal resources in the effort.
- *Financial costs*. Fines for not complying with important regulatory organizations' mandates can be steep. For example, penalties for willful violations of HIPAA requirements start at $1,000 per violation and can soar up to $50,000. A violation of the FERC Standards of Conduct recently cost one company over $2 million, in part for data loss.
- *Legal consequences*. The hefty fines described above may also be accompanied by criminal sentences, not to mention by potential legal action from parties who may have been injured by a company's failure to comply.

Depending on how you look at it, compliance is a tough challenge that will wreak havoc on your business if you don't stay on top of it – or a chance to benefit your business by protecting against risk and preparing for opportunity.

> ***Depending on how you look at it, compliance is a tough challenge or a chance to benefit.***

Benefits of constant compliance

- *Reduced risk*. Data backup is a great example. If you urgently need a contract that had been attached to an email, or a legal document, or other document and it's been deleted, a reliable, easy-to-use backup solution will enable you to find and retrieve it quickly.
- *Uninterrupted operations*. Maintaining a strategy for ongoing compliance means that when an audit is announced, you'll be prepared to demonstrate compliance with very little additional effort.
- *Ready for opportunity*. If you're developing new relationships or other opportunities in highly regulated areas such as government or healthcare, compliance can give you a competitive edge over other contenders.

Operate with Confidence and in Compliance

The most obvious reason to back up data is, of course, to be able to restore information that's been deleted or compromised in some way. But the other, equally important reason is to keep organizations in compliance with the growing number of laws regulating how they ensure the availability of information.

> ***Data backup plays a critical role in compliance with many laws.***

Data backup plays a critical role in achieving compliance with many of these laws, whether it's data in on-premises systems or in the cloud. You may not see a specific reference to backup in a given regulation, but if you see references to retaining information and keeping it available, you can be pretty sure that backup is going to be involved – and that it's going to turn up in compliance frameworks that relate to that regulation.

By being aware of the role of backup in compliance, and being familiar with the frameworks that delineate backup requirements, you can be better prepared to leverage backup as part of a complete compliance strategy.

About Spanning

Spanning, an EMC company and a leading provider of backup and recovery for SaaS applications, helps organizations to protect and manage their information in the cloud. We provide powerful, enterprise-class data protection for Google Apps, Salesforce, and Office 365. Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world.

For more information

Learn more about Spanning and start a free trial at www.spanning.com/free-trial.