SPANNING
by EMC

9 Ways to Make Your Auditors Love You

VISIT WWW.SPANNING.COM TO LEARN MORE AND START A FREE TRIAL.

Compliance: The Quality Auditors Find Irresistible

There's nothing an auditor loves more than a company that's in compliance with the laws that govern how organizations manage information. But getting your auditors to love you isn't always easy - not with the veritable alphabet soup of regulations, requirements, and controls that you need to understand. There's COBIT for information availability, HIPAA in the healthcare industry, CCM in the cloud… the list goes on and on.

Don't let that intimidate you, though. This eBook is the guide you need to understand what auditors are looking for and how to win them over - especially when it comes to regulations around information security, which often require data backup in order to achieve compliance. We'll show you the benefits of complying, introduce you to a set of compliance frameworks that will help, and give you nine sure ways to make sure you're ready when auditors come calling. Do it right, and you'll discover true bliss in a state of constant compliance, with lower business risk and less audit drama.

Auditor Love Can Make You Happy

There are plenty of benefits to being in a state of blissful compliance, where you're passing every audit with ease.

Reduced risk

Having measures in place to comply with regulations can lower not only the risk that auditors won't find what they're looking for, but also your general business risk. That means less risk of a data loss incident, and less time and money wasted trying to recover what you've lost. It might even lower your blood pressure too, by protecting against the kind of disastrous breach that can ultimately result in huge fines, bad publicity, and the loss of goodwill.

Uninterrupted operations

Maintaining a strategy for ongoing, sustainable compliance means that when an auditor comes calling, getting ready won't be a big deal. Instead of having to pull everything together at the last minute in a big push to handle the audit, which interrupts everyone's everyday responsibilities until the process is complete, you'll be prepared to show compliance with little special effort. And with audits happening monthly or quarterly for many organizations, it helps to be ready all the time. Otherwise, you'll find yourself scrambling to prepare for the next audit even when the current one is still wrapping up.

> Maintaining a strategy for ongoing, sustainable compliance means that when an auditor comes calling, getting ready won't be a big deal.

Ready for opportunity

If you're eager for business opportunities in highly-regulated areas like government or healthcare, compliance can give you a competitive edge. For example, if a government contract for which you're competing requires backup of cloud-based data and applications, and you already have such a system in place for compliance reasons, then you're automatically set to meet those contract requirements.

The Price You Pay for Non-Compliance:

- Up to $50,000 for HIPAA violations
- Up to $5,000,000 for Sarbanes-Oxley violations
- Up to 20 years in prison

The Heartbreak of Non-Compliance

While compliance can mean important benefits for your organization, non-compliance can bring some unpleasant consequences.

Failed audits

Failing a compliance audit isn't the worst thing. The real pain comes after you fail, when it's time to correct the problems that led to failure. Addressing the areas of concern in an auditor's report can take weeks or months - during which employees will be spending time correcting problems instead of focusing on building the business.

Financial costs

The cost of not complying with regulatory mandates can be steep. Penalties for willful violations of HIPAA, for example, can soar up to $50,000 for uncorrected violations. Under Sarbanes-Oxley, an executive responsible for willful, reckless violations can be personally fined up to $5,000,000.

Legal consequences

That $5,000,000 potential fine for violating Sarbanes-Oxley certification requirements may come with a prison sentence of up to 20 years. There can also be legal action from parties who have been injured by a failure to comply. For example, if your company mishandles a customer's sensitive data and they suffer a financial loss as a result, they may sue you to recover damages.

A Compliance Framework Is Your Best Friend

Compliance frameworks have emerged because the regulations governing information security don't always spell out the actions you need to take to be compliant. The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), for example, says you need to retain certain kinds of information for five years, but then doesn't explain specifically what to do to achieve that. A compliance framework is a collection of standards and controls that enable compliance. Meeting the standards and implementing the controls will put you in a better position to meet regulatory requirements.

In this context, you could say there are two kinds of compliance you need to be concerned about: compliance with the laws and regulations that apply to your organization, and compliance with the standards in the frameworks - since it's the latter that helps you by enabling the former.

The following frameworks are applicable to data stored in cloud (SaaS) applications:

Cloud Security Alliance (CSA)'s Cloud Controls Matrix (CCM)

As more companies move business applications and data off-premises, concerns have grown about ensuring compliance in the cloud. CSA's CCM provides a framework of controls aligned with several key security areas. Learn more here.

COBIT (Control Objectives for Information and Related Technology)

COBIT is a widely adopted framework that identifies 34 IT processes and 300+ control objectives to aid in achieving compliance with information availability requirements of a number of regulations. Learn more here.

NIST (National Institute of Standards and Technology) Recommended Security Controls

NIST's Recommended Security Controls for information systems pertain specifically to federal agencies and organizations that work with them. The controls assist organizations in complying with the Federal Information Security Management Act of 2002 (FISMA). Learn more here.

HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule

The HIPAA Privacy Rule, which is a part of the HIPAA regulatory requirements that cover many aspects of healthcare, functions as a framework within HIPAA. It delineates standards for compliance as well as implementation specifications for the standards. Learn more here.

AICPA (American Institute of CPAs) SOCs (Service Organization Controls)

The auditors who determine whether an organization is in compliance often represent accounting firms. The AICPA SOCs constitute a framework of accounting standards and controls that auditors can apply to their work. Learn more here.

9 Ways to Make Your Auditors Love You

1. Be ready for anything, anytime

For a long time, companies have seen a visit from an auditor as a hugely disruptive event that requires everyone in the company to stop what they're doing and scramble to make sure all the i's are dotted and t's crossed, so that the auditor will be happy with their compliance performance. But with quarterly or annual compliance cycles being the norm in so many companies, it's likely you know they're coming. So why not be ready? Try taking a proactive approach that makes audit preparedness part of your overall day-to-day culture, so that you're ready anytime an auditor announces a visit.

2. Embrace shadow IT

As you work toward compliance, it can be daunting to know that you may be talking about compliance for dozens and dozens of apps (Forrester puts the average at 66), including all those apps that people are using that aren't even officially sanctioned. These "shadow IT" apps have traditionally been labeled a security or compliance risk, but their existence can indicate that current policies are getting in the way of innovation. Even if you're concerned about critical data leaking out through these apps, consider embracing them instead of shunning them. When you think of them as something to be managed, rather than eliminated, you can begin to look at putting policies in place to identify them, evaluate them, apply appropriate controls to them, and make them openly available for people to use to work productively.

3. Make SPAR your priority

No, we're not suggesting that you duke it out with the auditors, rather that you focus on **Security, Privacy, Availability,** and **Reliability** - all those non-functional requirements of apps that are often overshadowed by the functional requirements. By giving these non-functional attributes priority status, and making them part of everyday conversations around security and compliance, it becomes possible to ensure that apps are addressing security and compliance as well as delivering functional value.

4. Create good policies and stick to them

Governance and security policies exist to help people manage the data that the applications must leverage. Establishing these policies is as straightforward as setting forth a collection of practices your company will adhere to in areas such as:

- employee onboarding and exiting,
- password rotation,
- secure coding standards,
- system access.

Codifying these into policies is the easy part; committing to applying them on a regular basis is tougher - but necessary.

5. Automate processes for sticking to policies

One way to stick to the policies you create is to automate the processes associated with applying those policies. Looks for apps with built-in tools and automation that will help you make sure you're following policies in a reliable, repeatable way. These tools include simple reminders, automated tests, checklists, and data archiving. For example, if a product can remind you to do a particular check or, better yet, if it can simply do it automatically for you, that will make it that much easier to stay safe and to scale.

6. Make sure your auditing firm is a good match

Choose your auditing firm very carefully. They'll be the partner who's there to lend help and support throughout the auditing process. When you're trying to figure out how your business practices map to the various frameworks' control matrices and the statements of attestation you need to follow, you want an auditing firm who can help you place all of that into the context of how your own organization works.

7. Store artifacts for everything, always

Storing artifacts for everything is part of taking a proactive approach to auditing, rather than rushing to react when you hear an audit's about to happen. It essentially means behaving as though somebody's always watching - instead of suddenly feeling put on the spot. Make it easy on yourself by providing a way to demonstrate anytime you're called up on to do so that you've done everything according to policy, exactly the way you said you would.

8. Check your checklist

This is the simplest technique you can imagine for making the audit process go your way: Write down what you need to do and when, and then verify that you did. It's a simple process of applying standard business practices - but an easy one to forget that you need to follow.

9. Choose your data backup solution well

If you use SaaS applications like Google Apps or Salesforce, protecting the critical data that you're storing in them is an important part of achieving compliance with information-security regulations. All the compliance frameworks we introduced earlier require data backup to be in place for compliance to be achieved, as summarized in the accompanying table.

What to Look for in a Backup Solution for SaaS Data:

- **Restore capabilities**, including accurate restore of point-in-time data into the app
- **Backup capabilities** with individual file protection (so that one error doesn't cause you to lose an entire backup
- **Backup status reporting** to help identify issues with backup and improve data quality
- **Automatic protection** for data whenever a new user is added
- **No storage limits**, to avoid running out of space for backups
- **Security certifications** such as TRUSTe Certified Privacy Seal or Skyhigh Cloud Trust
- **SSAE 16 Type II** audit completed by the backup provider
- **Data privacy protection** to ensure users only see data they're authorized to see
- **Alignment** with backup-related compliance frameworks

COMPLIANCE FRAMEWORK SUMMARY	
CSA's CCM Framework	CSA's CCM framework specifically includes a control that calls for backup and recovery measures to be incorporated and tested for effectiveness as part of business continuity planning.
COBIT Control Objectives	COBIT control objectives include one that states that a proper strategy for backup and restoration should be implemented (including developing and testing of a recovery plan) and one that provides guidance for activities such as backup recovery.
NIST Recommended Security Controls	NIST Recommended Security Controls include an Information System Backup control that specifically requires backups of user-level and system-level information (including system state information) contained in the information system.
HIPAA Privacy Rule	HIPAA Privacy Rule directs organizations to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information, as well as to establish procedures to restore any loss of data.
AICPA SOC	AICPA SOCs include an accounting standard that focuses on controls related to the ability to maintain rigorous operational and security of systems, with criteria including the existence of procedures for data backup, offsite storage, and restoration

Conclusion

Want to be an auditor's dream company, achieve full compliance, and live happily ever after? You can have it all, by cultivating a positive attitude about audits, getting plenty of support from compliance frameworks, and following the advice in this eBook.

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. Start a free 14-day trial at Spanning.com/try-it-now.

SPANNING by EMC

Follow us on Twitter @spanningbackup | Follow us on LinkedIn
Follow us on Google+ | Read our blog
www.spanning.com | +1 (855) 295-8111