



EBOOK

The Science of Compliance

Table of Contents

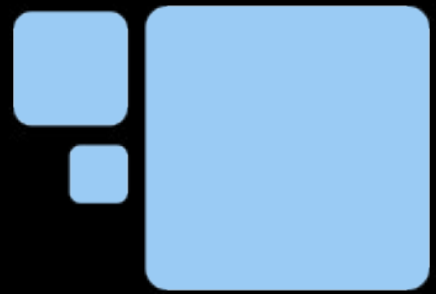
03 Introduction

07 HIPAA Compliance: Not Just for Doctors

12 Are You an Accountant? What You Should Know About SOX Compliance

16 Don't Swipe Another Card Until You're in PCI DSS Compliance

20 Let Our Company Run a Compliance Risk Assessment, So You Know Where You Stand



Introduction

Regulatory compliance: it's a subject no one likes to talk about, and yet – if your business isn't well-versed with it and takes measures to ensure compliance – it could be awful news.

Regulatory compliance is simply making sure that organizations are following their required state and federal laws, as well as all required standards and procedures. That may sound simple enough, but considering all the different federally mandated compliances out there, such as HIPAA, SOX, and PCI DSS, it can be easier than you think to fall out of compliance. And if that happens, you're looking at possible federally imposed fines, audits, and even public humiliation from the negative attention that comes with an investigation. The bottom line is: not staying within regulatory compliance will end up equating to significant lost revenue for your organization, and perhaps more.

What's "more"? According to Black Stratus, formal penalties for noncompliance with SOX can include fines, removal from listings on public stock exchanges, and invalidation of D&O insurance policies. That's a lot more. Hence, the reason regulatory compliance is often the very backbone of an organization's security system.



Regulatory Compliance Isn't Always an Easy Road to Follow

While there are many different types of regulatory compliance regulations for various industries, the three largest are HIPAA, SOX, and PCI DSS. Your particular organization may deal with only one or with all three. In any case, it's highly advised to familiarize yourself with the specific details of the regulations which apply to you.

That being said, it is, unfortunately, possible to believe you are taking all necessary measures to ensure comprehensive compliance, yet still unknowingly be in violation of one or more regulations. Some of the reasons for this may include referencing outdated materials, new wordings of rules replacing old, and basic misunderstanding of how each law is interpreted by enforcement agencies.

The bottom line is: not staying within regulatory compliance will end up equating to a significant loss of revenue for your organization, and perhaps more.



What Can You Do?

First and foremost, as you are the greatest watchdog for yourself and your business, you should begin familiarizing yourself with the most up-to-date information on regulatory compliance to the best of your ability. While some of your study materials may indeed quickly become obsolete, you will still know much about your specific compliance regulations, and can then take measures to stay updated on any changes.

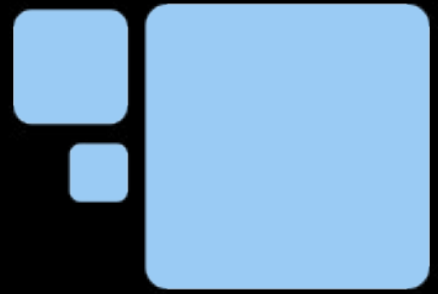
After that, it's time to get your technology in absolute compliance, and that means finding an IT support service with expert-level knowledge on regulatory compliance. Once we understand your exact needs, we will create a customized infrastructure for your organization that ensures strict regulatory compliance with your requirements, including HIPAA, SOX, and PCI DSS. If you're not too familiar with them, we've provided a starting place in this book for you to begin your education on each category.





CHAPTER ONE:

HIPAA Compliance: Not Just for Doctors



Just as the title above suggests – contrary to popular belief, doctors and hospitals aren't the only ones bound by HIPAA law. HIPAA was created in 1996 to ensure an individual's health record was theirs to share and theirs alone. Thereby, HIPAA law extends to any organization involved with an individual's medical records, including:

- Health Insurance Providers
- Doctors
- Clinics
- Hospitals
- Nursing Homes
- Dentists, Orthodontists, and Oral Surgeons
- Mental Health Specialists
- Pharmacies
- Any Business or Entity Sharing Medical Records with These Organizations



As such, HIPAA law enforces the obligation of these organizations to steadfastly protect the privacy, security, and accuracy of all medical records entrusted to them. We are vastly familiar with all aspects of HIPAA law, including the following aspects:

- **The HIPAA Privacy Rule** – sets limits on the handling and disclosure of any and all medical records without prior knowledge, understanding of, and approval from the patient. This rule also allows individuals to have access to their medical records to ensure complete awareness and accuracy of their contents.





- **HIPAA Compliance for Business Associates** – extends HIPAA law to cover not only the original definition of a “HIPAA-Covered Entity,” but also to any and all business associates with whom they share medical records. This newer aspect of HIPAA law ensures coverage over every organization who keeps medical records for any reason.
- **HIPAA Security Rule** – governs practices for how medical records may and may not be saved and shared. One of the largest undertakings in the medical industry as a result of this rule is the current universal conversion of all patient medical records from the original paper method to electronic data. As a result, organizations operating under HIPAA law must take austere measures to ensure strict HIPAA compliance with all medical data, leaving no stone unturned to minimize risk between data transfers and storage.
- **HIPAA Omnibus Final Rule** – the newest rule under HIPAA compliance law. According to Hitech Answers, the modifications within this rule are intended to:
 - Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules’ requirements.
 - Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
 - Expand individuals’ rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.



- Require modifications to, and redistribution of, a covered entity's notice of privacy practices.
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.



Is your organization adequately prepared to stay within HIPAA compliance law? Our company is.

HIPAA law extends to any organization involved with an individual's medical records.



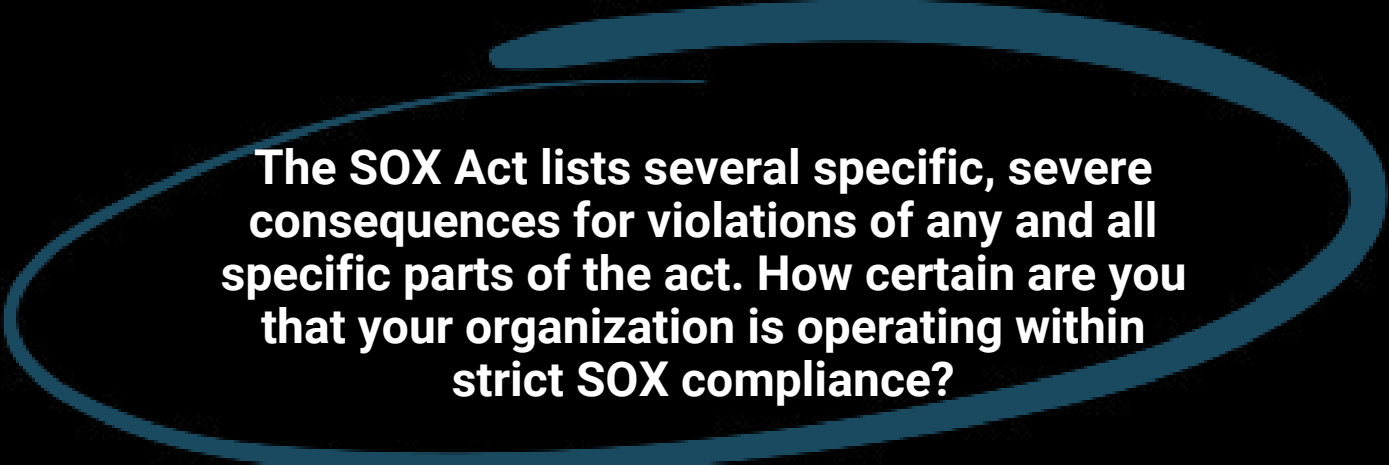

CHAPTER TWO:

Are You an Accountant? What You Should Know About SOX Compliance



The Sarbanes-Oxley (SOX) Act of 2002 mostly came about thanks to a great deal of national attention surrounding several financial and accounting scandals by major corporations in the mid-to-early 2000's. These corporations, such as Enron, Tyco International, AIG, Adelphia, Peregrine Systems, and WorldCom were discovered to have had executives within each organization who falsified accounting records to either secretly steal money for themselves, or to disguise decreasing company earnings, which falsely maintained higher company stock prices. As a result, most of the corporations either failed or were sold off, and left in their wake thousands unemployed and billions of dollars lost.

As a result, Congressmen Paul Sarbanes and Michael Oxley joined forces to create the SOX Act, creating an enforcement method with the goal of protecting shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improving the accuracy of corporate disclosures. There are many elements of SOX compliance, all of which we are very familiar with.



The SOX Act lists several specific, severe consequences for violations of any and all specific parts of the act. How certain are you that your organization is operating within strict SOX compliance?

A Brief Overview of the Major Elements of SOX Compliance:

- **Public Company Accounting Oversight Board (PCAOB)** – provides independent oversight of public accounting firms providing audit services, as well as enforcing registration of auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.
- **Auditor Independence** – establishes standards for external auditor independence to limit conflicts of interest, as well as addressing new auditor approval requirements, audit partner rotation, and auditor reporting requirements.



- **Corporate Responsibility** – mandates that senior executives take individual responsibility for accuracy and completeness of all corporate financial reports.
- **Enhanced Financial Disclosures** – sets enhanced reporting requirements for financial transactions, as well as requiring internal controls for assuring the accuracy of financial reports and disclosures.
- **Analyst Conflicts of Interest**– includes measures designed to help restore investor confidence in the reporting of securities analysts.
- **Commission Resources and Authority** – defines practices to restore investor trust in securities analysts, as well as the SEC's authority to censure or bar securities professionals from practice.
- **Studies and Reports** – require the Comptroller General and the SEC to perform various studies and report their findings.
- **Corporate and Criminal Fraud Accountability** - describes detailed criminal penalties for altering or destroying financial records, including any other interference with investigations, while providing certain protections for informants.
- **White Collar Crime Penalty Enhancement** - increases the criminal penalties associated with white-collar crimes and conspiracies.
- **Corporate Tax Returns** - states the Chief Executive Officer must sign company tax returns.
- **Corporate Fraud Accountability** - identifies corporate fraud and records tampering as criminal offenses, and lists to specific penalties for such offenses.

The SOX Act contains several specific, severe consequences for violations of any and all specific parts of the act. How certain are you that your organization is operating within strict SOX compliance? With our company, you will be quite certain, indeed.



CHAPTER THREE:

Don't Swipe Another Card Until You're in PCI DSS Compliance



PSI DSS stands for Payment Card Industry Data Security Standard, which was created by the world's major credit card companies to set credit data security standards so to reduce credit fraud. Any business, company or organization accepting credit card payments must conform to PSI DSS compliance.

Main Control Objectives for PCI DSS Compliance:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Enforcing strong access control measures
- Proactive and regular monitoring of your network
- Maintaining an updated information security policy



PCI DSS Compliance Ensures You're Covered, and Your Clients are Covered

Just as with HIPAA law, if your establishment processes, shares, or stores any credit or financial information, you are obligated to conform to governmental standards and take measures to ensure complete security of that information. Now, after reading that last sentence, if you're just a little more nervous about the safety of your current system -- don't fret. Our company is here to help. We'll be more than happy to come in, review your current security measures (or the lack thereof), and make immediate recommendations to get you back into full PCI DSS compliance.

Act Before It's Too Late

So, how can our company help you if your organization has already suffered a data breach? Well, to be perfectly honest, we can't. Truthfully, once a data breach has already occurred, the damage is done. You now have the unenviable task of informing your customers about the breach, trying to calm their anger and fears, trying to stay afloat with the loss of business and your reputation, reporting the breach to the proper authorities and, in turn, prepare to pay the imposed fees and fines.

Now, how can we help you if your organization has not yet suffered a data breach? Plenty! We will formulate a security framework customized to your exact needs that will make your data virtually impenetrable.



Fines and Retributions Associated with Non-PCI DSS Compliance are No Fun

Why do we stress the importance of full PCI DSS compliance? Oh, we'll show you. Let's take a quick peek at a few of those lovely fines and retributions you'll likely be slapped across the face with if your breach is determined to be due to your organization operating in non-PCI DSS compliance:

- Fines of up to \$500,000 per incident for security breaches
- Suspension of credit card acceptance by a merchant's credit card account provider
- Cost of lost business during store closures, business discontinuity, and processing time
- Possible civil litigation from breached customers
- Loss of reputation with their clients and partners
- Loss of customer trust, affecting future revenue


Outsmart the Hackers Before They Outsmart You

The term "hacker" used to mean a criminal who is highly skilled in computer programming and dubious Internet access. Nowadays, the "highly skilled" part isn't even required. Indeed, many underground websites have step-by-step instructional videos for would-be "hackers" that can teach them to break into almost any company website and access their data. It's becoming that commonplace. In fact, it's gotten so bad that, in recent years, the FBI has even placed cyber security near the top of their priority list. Don't you think if the hackers and the FBI are prioritizing data breaches, your organization should, too?



CHAPTER FOUR:

**Let Our Company Run a
Compliance Risk Assessment, So
You Know Where You Stand**



It is our great hope that you have reviewed this eBook and learned about the risks of noncompliance with HIPAA, SOX, and PCI DSS laws, you now understand the absolute necessity of prioritizing your data's most sensitive security. In truth, even organizations who believe they have every security protocol in place are shocked after a Compliance Risk Assessment is run and they discover holes in their security system. And usually, these are holes that hackers are well familiar.

Give us a call, and after our Compliance Risk Assessment, we'll show you how we'll plug all those holes before a would-be hacker even has a chance to exploit them. Our goal is to have any potential computer criminal visit your site, attempt any and all methods of breaking in, and finally leave in disgust because your fortifications are simply too strong. We will make your website into a veritable Fort Knox -- locked-up tight, safe and secure.



Intelligent Automation, LLC
5 Big Island Road
Warwick, NY 10990

<http://intelamation.com>
+1 (888) 711-4521