



# An Introduction to Regulatory Compliance

Regulatory compliance isn't the most interesting topic to talk about, but it is far too important to neglect. Considering that compliance infractions can result in hefty fines or jail time, staying up-to-date on current and future compliance changes are integral to a functioning business.

So what does regulatory compliance mean?



Essentially, being compliant means that you are adhering to the laws, regulations, and guidelines of the field you are doing business in. With so much important and classified data becoming electronic these days, it's crucial that there are rules to follow to make sure personal information and intellectual property are protected.

## The Basics of Regulatory Compliance

There are various regulatory compliance laws. Three of the most relevant are [HIPAA](#), [SOX](#), and [PCI](#):

**HIPAA** - These are the regulations impacting everything related to health care and patient information. The Health Insurance Portability & Accountability Act (HIPAA) demands that attention, resources, and money from the host organization are used to protect highly sensitive and personal health data.



HIPAA violations can get very expensive. Violations are typically caused by negligence on the part of the organization, and the penalties for non-compliance can range from \$100 to \$50,000 per violation, with a maximum penalty of \$1.5 million per year for repeated violations.

**“If a business isn’t compliant, it’s very likely that their reputation and customer trust could become damaged beyond repair.”**

**SOX** - This is the regulation that protects financial information. The law that enabled this regulation, the Sarbanes-Oxley (SOX) Act of 2002, is a United States federal law that was passed in response to a number of major corporate and accounting scandals. This compliance is here to make sure no one takes advantage of your highly secretive banking information, also covering issues such as auditor independence, corporate governance and enhanced financial disclosure. You can trust accounting and reporting practices again.



SOX violations can also get very expensive, reaching upwards to [\\$5 million in fines and 20 years in prison](#).

**PCI DSS** - This regulated the handling of credit card information. The payment card industry (PCI) is made up of credit card companies such as Visa, MasterCard, and Discover, who came together to create industry requirements to reduce theft and fraud of card information.



Violations of this regulation can reach up to [\\$100,000 monthly](#). Yikes.



## What Can Happen If You're Non-Compliant

As previously mentioned, in addition to getting heavily fined and possibly jailed, non-compliance can result in an immense loss of trust and confidence from your clients, and that kind of damage is almost impossible to recover from. If your business handles any personal information, compliances need to be met 100% of the time. That means finding someone who knows the compliance standards inside and out and is capable and adequately protecting personal information.



We will help your company always meet regulatory standards and puts security at the forefront.

## How We Will Keep You Compliant

Our staff is always informed and educated on the ever-changing security standards for your business. We will also regularly run risk assessments of your IT to make sure that you never fall under compliance standards. This will expose any potential risks you might be subject to and address them right then and there, giving you the peace of mind to keep working.

Think your business needs a partner to get your compliance in order? Get in touch! We'll take care of you.

**Contact Us**

[www.insitenet.net](http://www.insitenet.net)

415-787-4164

201 Spear Street, Suite 1100  
San Francisco, CA 94105