Information Security Compliance: Which regulations relate to me?

Tags: compliance, Cybersecurity, Eric Vanderburg, FERPA, FISMA, GLBA, HIPAA, information security, payment card industry, pci, pci-dss, regulation, SOX

21 December, 2020

Information Security Compliance Learning Objectives:

reading this article, you will have a better understanding of:

Different compliance regulations;

What they regulate; and

Which companies / industries are affected.

Speak to a Security Expert

Related Articles:

nformation Security Compliance: HIPAA

ctives | Compliance Regulations | Assessing Regulations | Conclusion | Regulations Table | Get Started

ssing which rules and regulations apply to an organization is no easy feat. Often, organizations need to comply with multiple frameworks and overlapping qualities.

is article, we attempt to demystify common cybersecurity frameworks and regulatory requirements to help organizations initiate discussions pliance.

entry is part of a series of information security compliance articles. In subsequent articles we will discuss the specific regulations and cyberse ribing their precise applications. These include, but are not limited to:

- NIST (National Institute of Standards and Technology)
- CIS Controls (Center for Internet Security Controls)
- ISO (International Organization for Standardization)
- HIPAA (Health Insurance Portability and Accountability Act) / HITECH Omnibus Rule
- PCI-DSS (The Payment Card Industry Data Security Standard)

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- AICPA (American Institute of Certified Public Accountants)
- SOX (Sarbanes-Oxley Act)

- COBIT (Control Objectives for Information and Related Technologies)
- GLBA (Gramm-Leach-Bliley Act)
- FISMA (Federal Information Security Modernization Act of 2014)
- FedRAMP (The Federal Risk and Authorization Management Program)
- FERPA (The Family Educational Rights and Privacy Act of 1974)

- ITAR (International Traffic in Arms Regulations)
- COPPA (Children's Online Privacy Protection Rule)
- NERC CIP Standards (NERC Critical Infrastructure Protection Standards)

; to Top

Many fear information security as an amorphous issue that only the IT department handles. The reality is that the legal and reputational ramifications that ensue from a data breach affect the entire organization. That is why it is essential to create a security-centric culture, top to bottom, with a focus on complying with information security regulations.

Compliance Regulations

Regulations are in place to help companies improve their information security strategy by providing guidelines and best practices based on the company's industry and type of data

Part of that difficulty is because regulations are not written in a way that can be easily understood by the average person. Often, partnering with a security professional is necessary to decode relevant requirements and devise an implementation plan. These professionals have experience implementing systems, policies, and procedures to satisfy the requirements of various regulations and enhance the security of an organization. Many have obtained credentials, such as the **HISP (Holistic Information Security Practitioner),** that signifies they have a deeper understanding of the system controls required to reach compliance.

Back to Top

Assessing Which Compliance Regulations Relate to an Organization

Regardless if a company chooses to engage a trusted advisor, the first step of the process is to assess which laws and acts apply to them. Once completed, they need to organize their information security to address the boundaries put in place by those acts. This process requires a set plan that outlines a consistent and effective way of alerting and dealing with threats.

Discussing specific legislation as it relates to individual companies can be vague. A **cybersecurity assessment** is a valuable tool for achieving these objectives as it evaluates an organization's security and privacy against a set of globally recognized standards and best practices.

Back to Top

Take for Example:

Think of a local hospital. This hospital is publicly traded and not a federal agency; therefore, it is not subject to the FISMA bill. It does deal with patients and other healthcare-related data, so it is subject to HIPAA.

With the regulation identified, the hospital must look carefully at what sort of protection it must offer patients and place safeguards in effect to prevent a breach of security. On the ground level, it cannot give away information without the express consent of the patient. From a more technological perspective, the hospital cannot allow any system that handles patient information to be compromised.

These guidelines require controls to be in place for those systems and the equipment that allows access to the systems. Policies and procedures need to be in place to govern the activities of personnel who interact with those systems, and training needs to occur, so users understand how to properly perform their duties without potentially misusing the system, intentionally or not.

While the example of the local hospital only had to comply with one regulation, companies often find they must meet the requirements of many regulations. In such cases, the best method to approach the situation is to outline all of the regulations that will impact the company first, and then determine which security controls need to be implemented to satisfy all of the requirements effectively. There are often overlapping requirements built into different regulations, so by breaking it down into two phases, companies can reduce the amount of time and money they would otherwise spend by reducing the duplicate effort of implementing competing systems.

This table shows the different cybersecurity frameworks and regulations, what they regulate, and which corporations would be subject to the scope of the act.

Back to Top

Do You Have Questions About Frameworks, Regulations, or Compliance?

There is an abundance of laws and bills on the books designed to protect information. However, it is not always clear to the average business decision-maker which regulations apply to their organization. That is where **a security professional can significantly help** a business make sense of such an area that grows more complex with each new regulation. Compliance is critical, and it begins by understanding which regulations affect your company and then outlining the steps to bring you into compliance.

Get Started Today

Back to Top

First Name*

Last Name*

Company*

Business Email*

Direct Phone*

GET STARTED

Eric Vanderburg See More Articles

Share Article:

education he worked as a consultant specializing in the development and maintenance of information management and network security systems for businesses, law firms, and government agencies. He was a professor of computer networking at Remington College where he taught courses on information security, database systems, and computer networking and has been invited to speak at many organizations and campuses on technology and information security.

Greensboro, North Carolina
4508 Weybridge Lane
Greensboro, North Carolina 27407
Tel +1.888.823.2820

Cleveland, Ohio
The Idea Center, Playhouse Square
1375 Euclid Ave — Suite 400
Cleveland, OH 44115
Tel +1.216.664.1100

SIGN UP