IJCS

INTERNATIONAL JOURNAL OF

CYBER SECURITY

Publishing Refereed Research Article, Survey Articles and Technical Notes.

Journal ID: 2145-6523

IAEME Publication
Chennai, India
editor@iaeme.com/ iaemedu@gmail.com

https://iaeme.com/Home/journal/IJCS

International Journal of Cyber Security (IJCS)
Volume 3, Issue 2, July-December 2025, pp. 1-9, Article ID: IJCS_03_02_001
Available online at https://iaeme.com/Home/issue/IJCS?Volume=3&Issue=2
Impact Factor (2025): 2.40 (Based on Google Scholar Citation)
Journal ID: 2145-6523; DOI: https://doi.org/10.34218/IJCS_03_02_001

SECURITY COMPLIANCE STANDARDS

Yashwant Shukla
Dominion Energy Service Inc, Cayce – SC, USA.

ABSTRACT

This paper provides a detailed look at the important security compliance standards that exist in different industries, stressing the need for creating specific security plans to tackle the unique issues each sector faces. As our world becomes more connected, industries are increasingly depending on strong cybersecurity measures to protect sensitive data and meet legal requirements. Every industry has its own compliance standards that are tailored to fit its specific needs. These standards are crucial for helping organizations manage risks, safeguard data, and build trust with their stakeholders. This paper focuses on the main compliance standards that are vital for six key industries: healthcare, finance, SaaS software, manufacturing, government, and energy utilities. These standards are designed to protect patient data and ensure that strong information security management systems are in place. The paper also investigates the compliance standards for other industries, emphasizing the need for customized security strategies to meet the specific challenges they encounter.

Keywords: Security Compliance, Cybersecurity, Data Protection, Risk Management, Healthcare, Finance, SaaS, Manufacturing, Government, Energy Utilities.

Cite this Article: Yashwant Shukla. (2025). Security Compliance Standards. *International Journal of Cyber Security (IJCS)*, 3(2), 1-9.
https://doi.org/10.34218/IJCS_03_02_001

1. Introduction

Security compliance is a major component of cyber security and event Security compliance can be further segmented in various categories.

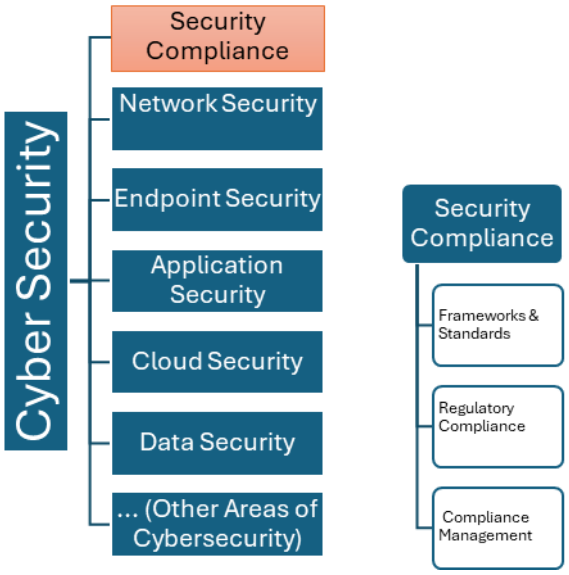

Figure 1: Security compliances on high level in Cyber security

In the field of cybersecurity, security compliances hold a great importance. Our security standards play a big role in ensuring that you stick to the right security practices, which helps avoid any security issues. When we create security standards for any systems, we rely on tried-and-true practices that have been tested by many knowledgeable experts in the field. These industry standards get developed over time, taking into account various factors to ensure that the minimum recommended security measures are met without spending too much money and time.

One of the biggest challenges when implementing security for any system is making it efficient. You can add all sorts of security measures, but sometimes those measures might not be necessary for that specific system. This can lead to extra costs, delays, and even create annoying security layers that frustrate users.

For instance, think about locks: you wouldn't use the same lock for your home as you would for a bank vault. The bank vault needs a more complex lock because it protects more valuable assets. Similarly, different systems require different security standards based on their specific needs. There are many well-known security standards recommended by organizations like CISA, which work with experts who understand the systems closely. They can assess what extra security is needed based on the costs and potential threats. When designing or working on

a system to enhance its security, it's always a good idea to follow common security principles and use some common sense. Sticking to the recommended security standards for that specific system domain is essential.

Next, we will discuss some major security standards and compliance requirements.

2. Major Security and Compliance Standards

- **TSA**: The Transportation Security Administration (TSA) is a federal agency that provides security screening for air travelers in the U.S. and implements security directives for various sectors, including pipeline security
- **PCI**: The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment
- **FISMA**: The Federal Information Security Modernization Act (FISMA) is a U.S. law that requires federal agencies to protect their information and information systems from unauthorized access and disruption by implementing security guidelines and standards
- **HIPPA**: The Health Insurance Portability and Accountability Act (HIPPA) provides data privacy and security provisions for safeguarding medical information, ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI)
- **ISO/IEC 27001**: The International Organization for Standardization (ISO) is an independent, non-governmental organization that develops international standards to ensure quality, safety, and efficiency across various industries
- **NIST SP 800-53**: The National Institute of Standards and Technology (NIST) is a U.S. government agency that develops and promotes measurement standards, including cybersecurity guidelines
- **NERC CIP**: The North American Electric Reliability Corporation (NERC) is a regulatory authority responsible for ensuring the reliability and security of the North American bulk power system
- **GDPR**: GDPR security compliance involves implementing measures to protect personal data and privacy of EU residents, ensuring adherence to regulations and safeguarding sensitive information.

- **SOX**: The Sarbanes-Oxley Act, which mandates strict financial reporting and auditing requirements.
- **CSA STAR**: The CSA STAR (Security, Trust, Assurance, and Risk) is a certification framework developed by the Cloud Security Alliance that provides assurance in cloud security through comprehensive auditing and certification
- **CIS Controls**: A set of best practices for securing IT systems and data.

In today's interconnected world, industries are increasingly reliant on robust cybersecurity [1] frameworks to protect sensitive data and ensure compliance with regulatory requirements. Different sectors have unique compliance standards tailored to their specific needs. This paper explores the key compliance standards across six major industries: healthcare, finance, SaaS software, manufacturing, government, and energy utilities.

2.1 Compliance Standards Overview

Compliance standards are established guidelines and practices that organizations must follow to ensure the security and privacy of data. These standards help mitigate risks, protect sensitive information, and maintain trust with stakeholders. Below, we define the sets of compliance standards relevant to each industry.

2.2 Healthcare Industry

The healthcare industry is subject to stringent regulations due to the sensitive nature of patient data. The key compliance standards for healthcare include:

- ISO/IEC 27001
- NIST SP 800-53
- HIPAA
- GDPR
- CIS Controls

2.3 Finance Industry

The finance industry handles highly sensitive financial information and is subject to multiple regulatory requirements. The key compliance standards for finance include:

- ISO/IEC 27001
- NIST SP 800-53
- PCI DSS
- GDPR
- SOX
- CIS Controls

2.4 SaaS Software Industry

The SaaS (Software as a Service) industry focuses on delivering software applications over the internet. Key compliance standards for SaaS software include:

- ISO/IEC 27001
- GDPR
- CIS Controls

2.5 Manufacturing Industry

The manufacturing industry, while not traditionally associated with data security, increasingly relies on digital systems. Key compliance standards for manufacturing include:

- ISO/IEC 27001
- GDPR
- CIS Controls

2.6 Government Sector

The government sector deals with a vast amount of sensitive information and is subject to rigorous security standards. Key compliance standards for government include:

- ISO/IEC 27001
- NIST SP 800-53
- FISMA
- GDPR
- CIS Controls

2.7 Energy Utilities Industry

The energy utilities industry is critical to national infrastructure and requires robust security measures. Key compliance standards for energy utilities include:

- ISO/IEC 27001
- NIST SP 800-53
- GDPR
- CIS Controls

2.8 Comparative Analysis

A comparative analysis of the compliance standards across these industries reveals several commonalities and differences. **ISO/IEC 27001**, **GDPR**, and **CIS Controls** are universally applicable across all six industries, highlighting their broad relevance and importance. **NIST SP 800-53** is also widely adopted, particularly in sectors with stringent security requirements such as healthcare, finance, government, and energy utilities.

Industry-specific standards such as **HIPAA** for healthcare, **PCI DSS** and **SOX** for finance, and **FISMA** for government underscore the unique regulatory landscapes each sector navigates. These standards address the specific risks and challenges inherent to each industry, ensuring tailored protection measures.

Figure 2: Understanding Major compliances and applicable sectors

3. Segments of Security Compliances

Security compliances explained above can be further segmented on basis of their usages and way.

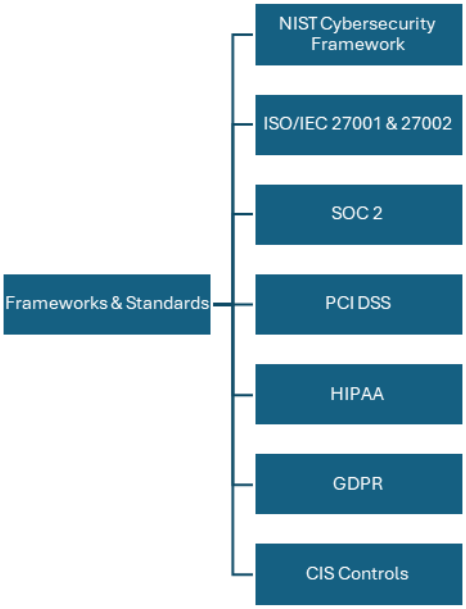

Figure 3: Frameworks & Standards

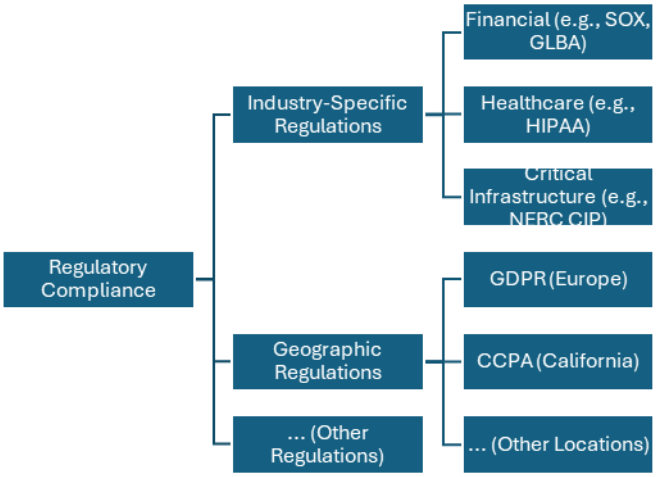

Figure 4:Regulatory Compliance

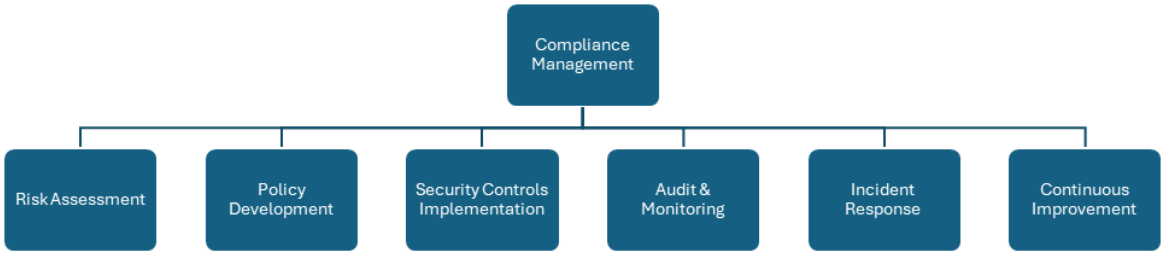

Figure 5: Compliance Management

4. Legal enforcement agencies behind these security compliances

We understand that it can be challenging to ensure people adhere to security compliances or any restrictions. Teaching them how to perform their jobs while following these guidelines can be difficult because people often desire the freedom to do things their own way. For any tasks they are undertaking, compliance is essential. However, without law enforcement or legal pressure, it becomes very difficult to enforce these rules.

So many of these security compliances are enforced by registered agencies which perform various audits and security checks to make sure these security compliances are followed. And in case of any misconduct or ignorance to these standards there is strict legal

action enforced by these agencies [1]. Some of these involve heavy fine and license revocation and some even involve prison too.

4.1 Financial Implication due to compliances

We've talked about the legal problems that can happen when companies don't follow rules, but there's also a money side to it.

Following security rules can cost companies some money. But not following them can cost a lot more.

There are two big ways companies lose money when they don't follow the rules:

1. They can get caught during audits and have to pay big fines.
2. If they skip important security checks and someone hacks their system, it can lead to a data breach.

When that happens, companies might have to deal with lawsuits from lots of people. Sometimes, the costs are so high that the company could go bankrupt.

For example, [2], Meta was fined $1.3 billion for breaking GDPR rules by sending customer data without proper protection.

5. Conclusion

Understanding the compliance standards relevant to each industry is crucial for organizations to safeguard their data and maintain regulatory compliance. By adhering to these standards, industries can enhance their security posture, protect sensitive information, and build trust with stakeholders. As the digital landscape continues to evolve, staying informed about compliance requirements will remain a key priority for all sectors. It gives a sense of trust to the consumers if the company of organization they are dealing it follows security compliances recommended for its industry. And legal support to these agencies helps ensuring these standards are implemented properly without any loose ends. Day by day technology is evolving for example we are not very far from quantum computing [4], and it will make data decryption easier. So in order to stay safe security compliances become very critical to make sure we are always ready and updated with newer threats.

Reference

[1] N. S. Blog, "News Blog," 05 12 2024. [Online]. Available: https://www.nri-secure.com/blog/us-cybersecurity-laws-compliance#:~:text=Major%20U.S.%20Cybersecurity%20Regulations%20and,NERC%20CIP%20%28Critical%20Infrastructure%20Protection%29.

[2] vinugayathri-chinnasamy, 04 07 2025. [Online]. Available: https://www.indusface.com/blog/cost-of-compliance-vs-non-compliance/.

[3] Y. Shukla, "Decrypting the Future: Quantum Computing's Role in Modern Cryptography," ijarcce.com, vol. 13, no. 8, pp. 252-261, 2024.

[4] Y. Shukla, "ESSENTIAL CYBERSECURITY: PROTECTING YOUR BUSINESS AND YOURSELF," INTERNATIONAL JOURNAL OF INFORMATION SECURITY (IJIS), pp. 23-38, 2025.

Citation: Yashwant Shukla. (2025). Security Compliance Standards. International Journal of Cyber Security (IJCS), 3(2), 1-9.

Abstract Link: https://iaeme.com/Home/article_id/IJCS_03_02_001

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCS/VOLUME_3_ISSUE_2/IJCS_03_02_001.pdf

✉ **editor@iaeme.com**