Demystifying Regulatory Compliance

for Security Leaders and IT Decision Makers

Introduction

The development of regulatory frameworks and standards has emerged from the need to address the challenges and requirements in managing information technology and safeguarding data. These frameworks and standards have not only evolved over time, but they have been shaped by technological advancements and emerging cybersecurity threats. The development of frameworks and standards has been primarily driven by the following factors:

- **Regulatory bodies** are emphasizing the need for organizations to be accountable for their cybersecurity practices and to comply with specific standards and regulations.
- **Advanced cyberthreats** are becoming more frequent and damaging. Often encompassing the sophistication that was once confined to state-sponsored threats but are now in the hands of opportunists and hacktivists.
- **Critical infrastructure and essential services** (e.g., healthcare, energy, finance) that are vital to the functioning of society and the economy. This includes federal legislation, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) of March 2022.
- **A lack of uniformity** in cybersecurity practices across different sectors and regions. Inconsistent approaches can lead to gaps in security and compliance challenges.
- **The executive order** on improving the nation's cybersecurity that was passed by the United States President in May of 2021.

It is clear that organizations need to be resilient in the face of cyberthreats, ensuring they can continue to operate and recover quickly from disruptions. With the growing amount of personal data being collected and processed, there is a heightened need to protect this data from cyberthreats and data breaches. Cyber incidents not only have a significant economic impact, leading to financial losses and undermining trust in digital services for the broader economy, but in some cases can cost lives, especially where the healthcare industry has been targeted.

Regulatory compliance is crucial for building organizational resilience. Companies that grasp the full scope of their risks recognize that compliance isn't just a checkbox activity, but a fundamental part of an overall security strategy. By adhering to regulations and implementing security best practices, organizations can better position themselves to withstand and quickly recover from most cyber incidents. This approach ensures that when a crisis hits, the groundwork for rapid recovery is already in place.

1.

Cyberattacks

If a company's digital infrastructure is under attack, the effects can go much further than just loss of data. The impacts of downtime, loss of core functions, potential disruptions to sales, and how the organization is perceived are all potential outcomes of a cyber incident.

In the wake of these possibilities, the impact on human life is the most important factor to keep in mind. Within financial service industries (FSI) and healthcare (HC) industries, cyberthreats can have life-altering impacts on individual levels with impact to bills, payments, and access to medical care among other critical services. Concerns and risks like these are a good reason for organizations to improve their security posture by following compliance within their industry regulations.

Why Compliance Matters

Compliance involves adhering to laws and regulations that apply to the organization's industry and geography. Being complaint can help reduce the impact to your business, from loss of revenue because of ransom payments to operational disruption, data breach exposures, regulatory fines, and reputational damage. Compliance standards are changing rapidly and will continue to do so. Regulations developed today to meet current objectives may not work in the future. Keeping with up the new frameworks and regulations and their new expectations is a surefire way to protect your organization.

Regulations vs. Frameworks

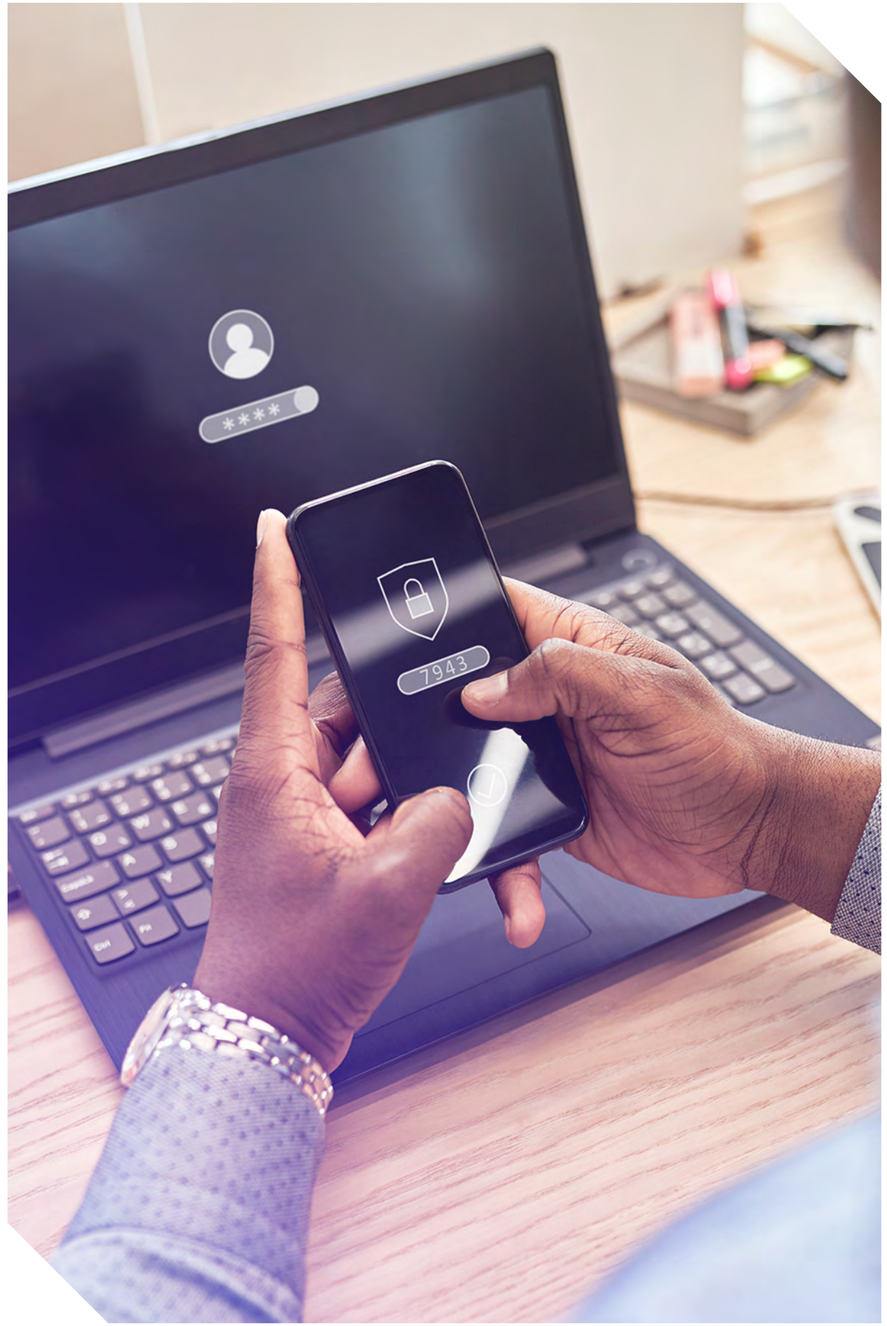
The core difference between regulations and frameworks is what you are trying to accomplish. Frameworks provide a structured set of guidelines, best practices, and standards that organizations can use to manage and improve their cybersecurity posture. Differently, regulations are legal requirements imposed by governments or regulatory bodies to enforce a minimum standard of cybersecurity practices across organizations. Some widely used regulations include:

- **GDPR** (General Data Protection Regulation) — European Union regulation for data protection and privacy.
- **HIPAA** (Health Insurance Portability and Accountability Act) — U.S. regulation for protecting healthcare information.
- **SOX** (Sarbanes-Oxley Act) — U.S. regulation for financial practices and corporate governance.
- **PCI DSS** (Payment Card Industry Data Security Standard) — Standards for securing credit card transactions.
- **FISMA** (Federal Information Security Management Act) — U.S. law for protecting government information.

Regulations like these work in tandem with frameworks. For example, frameworks provide the foundation for compliance with regulations, and regulations drive the adoption of frameworks. Frameworks also help organizations go beyond minimum regulatory requirements and facilitate easier compliance and auditing while regulations ensure consistent baseline security across sectors. Some widely used frameworks include:

- **NIST Cybersecurity Framework (CSF)** — Provides a comprehensive approach to managing cybersecurity risks.
- **CIS Controls** — A set of best practices to defend against cyberthreats.
- **COBIT** — Provides a framework for IT management and governance, with a strong focus on control objectives for IT, including cybersecurity.

Frameworks provide best practices for managing cybersecurity, while regulations enforce minimum standards to ensure baseline security across sectors.



Risk Management and Compliance

A risk-based approach begins with a thorough risk assessment. This process should involve input from various stakeholders, including security teams, IT personnel, legal experts, and business leaders.

For example, a healthcare provider may identify the protection of electronic health records (EHRs) as a top priority due to the sensitive nature of the data and the potential consequences of a breach, such as loss of patient data and regulatory fines under HIPAA. By prioritizing EHR security, the provider can focus its compliance efforts on implementing controls that mitigate the most significant risks.

As regulatory requirements continue to grow in complexity, organizations are increasingly turning to governance, risk management, and compliance (GRC) tools to streamline their compliance processes, enhance visibility, and ensure continuous monitoring and improvement.

A risk-based approach to compliance tailors security efforts to the unique risks of each organization, ensuring critical threats are prioritized.

Overview of GRC Tools and Their Benefits:

GRC tools are designed to help organizations automate and manage various aspects of compliance, including policy development, risk assessments, audit tracking, and incident response. These tools offer several key benefits:

- **Centralized compliance management:** GRC tools allow organizations to consolidate compliance activities into a single platform.
- **Automation of compliance tasks:** By automating routine compliance tasks, such as monitoring access logs or generating audit reports, GRC tools free up valuable time.
- **Enhanced visibility and reporting:** GRC tools providwe real-time visibility into compliance status, making it easier for security leaders to track progress, identify gaps, and demonstrate compliance to regulators and auditors.
- **Continuous monitoring and improvement:** GRC tools support continuous monitoring of compliance activities, enabling organizations to identify and address issues proactively rather than reactively.

2.

Why It Is Important to Adopt Compliance Regulations

The point of understanding your organization's risks and how you can account for them is not to find faults. Rather, it is important to find facts so that you can help your organization protect and move forward. While executives might think that their organization is prepared and would be cyber resilient, the reality could be very different — putting organizations at risk.

Ensuring there is board-level involvement and commitment is the main way to achieve compliance. Organizations need to foster a culture of compliance throughout the organization to reduce risk. Management is responsible for implementing processes and technology according to regulations. It is important to take a step back and make sure laws and regulations are followed in the context of the company's industry and geography.

As the industry continues to grow and change so too will what compliance and regulation standards look like. However, you don't want your company to fall behind in their compliance because then you'd risk becoming negligent, and that's when an executive or board member is liable to punitive measures. There could be financial penalties and reputational damage from an outage or a ransomware attack. But the more mature your organization becomes in terms of meeting the different regulatory compliance, the better chances of being able to recover rapidly.

Compliance Across the Globe

Around the world, if you look at cyber legislation, there are a total of over 150 countries with some sort of cyber legislation in place. Some of these include DORA in the EU, as well as NIS/NIS2 in the UK. Japan has FSA and the Middle East has NESA and DIFC Data Protection Laws. Globally, countries can look to NIST. When people in the U.S. think of ransomware and regulatory fines, they think of the Security and Exchange Commission (SEC). Despite the wide range of regulatory options, fewer than 100 countries have critical infrastructure regulation. This shows that a lot of countries aren't dealing with security at a high level even though there is a very real need to focus on these critical infrastructure environments. Looking at the healthcare industry specifically and including research and biotech, they often have different rules by country.

Compliance regulations ensure that your organization is prepared for cyber incidents, with board-level involvement crucial for fostering a culture of security.

veeam

How Financial Services and Healthcare Industries Differ

In the U.S., The Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) lists 16 critical industries that must be complaint with different regulations. When people think of critical industries, they normally think of dams, power grids, and obviously, healthcare. Healthcare and financial services play a critical role in the day-to-day lives of people across the globe. When looking at the negative effects that a lack of security compliance could have on healthcare organizations, the impact affects people's lives.

HIPPA is one of the main regulations that comes to mind when people think of healthcare compliance. The HIPAA Privacy Rule establishes national standards for the protection of certain health information while the HIPAA Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. If a healthcare provider is not properly protected or compliant, they could risk their patient data being compromised in the event of a ransom attack.

In the financial industry, one of the main regulations is GLBA, or the Gramm-Leach-Bliley Act. This act requires financial companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data. When a financial company is non-compliant with frameworks or regulations, they run the risk of facing potential costs such material financial losses, fines, economic stability, and reputational damage.

Organizations must continuously adapt to new regulations to maintain compliance and stay ahead of evolving cybersecurity threats.

3.

Best Practice Recommendations and Implementation

Compliance is far from a one-time consideration. Regulatory requirements are not static; they evolve over time as new threats emerge and regulations are updated. As such, there are some best practices to implement to ensure your corporation is staying on top if all crucial frameworks and regulations.

Continuous Monitoring

Continuous monitoring is a critical component of effective compliance management. GRC tools facilitate continuous monitoring by integrating with existing security infrastructure, such as SIEM (Security Information and Event Management) systems, to track compliance in real-time.

For example, a financial services firm subject to SOX may use a GRC tool to continuously monitor access to financial systems, ensuring that only authorized personnel have access to sensitive financial data. By integrating GRC tools into their cybersecurity strategies, organizations can streamline their compliance efforts, reduce the risk of non-compliance, and ensure that their security practices evolve in tandem with regulatory requirements.

Regular Audits and Assessments

During an attack it will not come down to if you have an incident response plan in place. You must *know* your plan will work. One of the best ways to ensure this is through testing. Testing your organization's plan and demonstrating that the test was successful is how you ensure the level of compliance.

Key Steps for Compliance

When looking at what regulations organizations can implement to become complaint it is important to take a wholistic approach. Every part of your organization can touch another aspect of your environment. Planning and forethought will play a huge role in assuring your organization's compliance. Some steps to consider include:

- **Develop a risk management process:** This involves identifying all potential IT risks that could affect your business as well as assessing your vulnerabilities.
- **Analyze and prioritize your risks:** This can be done through developing a risk mitigation strategy and training your staff.
- **Develop an incident response plan:** In this plan, you can consider things like risk transfer while maintaining visibility and insight of your environment.
- **Establish a culture of security:** This can look like involving all relevant stakeholders, picking the right technologies, and never forgetting to document, document, document.

Develop a risk management process, prioritize risks, and establish a culture of security to maintain compliance and enhance resilience.

Conclusion

The future of regulatory compliance will focus on resilience, with organizations needing to anticipate new regulations and build adaptable, proactive compliance programs.

The regulatory landscape is dynamic, and the pace of regulatory change is unlikely to slow down, particularly as governments and regulatory bodies respond to the rapid advancements in technology. With that in mind, the direction is for organizations to adapt security frameworks and continue to meet regulatory compliance. A secondary goal would be standardization of security best practices to get to a point where organizations reach an acceptable security posture.

In conclusion, regulatory compliance is an ongoing journey that requires continuous effort, adaptation, and collaboration.

It is not enough to simply achieve compliance; organizations must strive to maintain and enhance their compliance programs in the face of evolving threats and regulations. Security leaders and IT decision-makers play a crucial role in this process, guiding their organizations toward a compliance strategy that is not only about avoiding penalties but about building a stronger, more cyber resilient organization. By integrating compliance into the fabric of the organization's operations and culture, and by staying informed and agile in the face of change, organizations can navigate the complexities of the regulatory landscape with confidence and success.