BLUE RADIUS CYBER
SECURITY ASSURED

EBOOK

Understanding IT Regulatory Compliance

https://blueradius.ai

Table of Contents

Introduction

Data is being generated, shared, and stored at an exponential rate, and businesses rely on technology more than ever to connect with customers and deliver products and services. The rise of IT in the business world has not been a slow burn — it's an explosion. And companies are struggling tokeep up.

Even now, both public and private organizations across industries all around the world fail to protect critical and sensitive data. With inadequate infrastructure, little to no training, and non-existent compliance regulations, business and customer information is extremely vulnerable. Security breaches, cyberattacks, and accidental data loss are not uncommon, causing significant financial and reputational harm to companies and their customers.

That is where regulatory compliance comes into the fold.

Governing bodies have unleashed a mountain of policies, procedures, and legislations that aim to standardize security and minimize risk. Now companies are faced with a new challenge — IT regulatory compliance management.

Regulatory Compliance

Businesses must not only safeguard and maintain information but also prove they have high-integrity systems in place that help achieve an acceptable level of protection. It's a time-consuming task that is easier said than done — even when many tasks can be automated.

In this eBook, we will give you the information you need to gain a foundational understanding of regulatory compliance, what it is, why it matters, and what happens when businesses fail to comply.

CHAPTER ONE:

What Is Regulatory Compliance?

Regulatory compliance refers to the activities undertaken by businesses that maintain and prove adherence to externally imposed regulations, laws, and guidelines. Compliance is achieved through two distinct assurances:

- Management of compliance within the company

- Management of the integrity of the system used to ensure and provide evidence for compliance

Today, every business is an IT business. The amount of data generated, transmitted, and stored is growing at an exponential rate. Every day, we produce quintillions of bytes of data, some of which contain personal or highly sensitive information. And that's information that we do not want to be accessed and used by a malicious actor with sinister intentions.

Think about the information you share with your bank, healthcare provider, insurance provider, or employer. In the wrong hands, this data could be used to steal your identity, transfer funds from your bank account, or infiltrate your business network. Often, cybercriminals are out to make money from stolen information.

IT compliance involves protecting digital information and controlling how it is gathered, stored, and shared (internally and externally). Businesses must enforce internal compliance functions, as well as satisfy external regulations that protect both the company and the end user.

CHAPTER TWO:

Why Is Regulatory Compliance Used?

The vast majority of companies operating in the US are subject to at least one external IT security regulation. Maintaining compliance is often compulsory, but while it can be time-consuming and limiting, it does benefit both the business and its customers.

Here are just some of the reasons why regulatory compliance is used.

Regulatory Compliance Enhances Security

Cybersecurity is not just a buzzword — it is an incredibly important facet of modern-day technology use. In short, cybersecurity involves the protection of computer systems, networks, and data from theft or damage. It also helps prevent the disruption of services these systems deliver.

By setting minimum standards within industries, regulatory compliance significantly enhances security across the board. This sets an expectation that protects both businesses and customers from data theft, mishandling, and loss.

Regulatory Compliance Reduces the Risk of Data Loss

Data is one of the modern-day company's most valuable assets. Enhanced security helps mitigate the risk of unauthorized breaches, which can be incredibly costly (on average, more than $1.6 million).

"Enhanced security helps mitigate the risk of unauthorized breaches, which can be incredibly costly (on average, more than $1.6 million)."

Regulatory Compliance Ensure Standardization

Big or small, public or private — no business is immune from compliance obligations. By standardizing specific requirements, all organizations are required to undertake the same precautions and risk mitigation strategies. This helps level the playing field and gives consumers the confidence to select a brand that best aligns with their values without sacrificing the safety of their data.

Regulatory Compliance Earns Customer Trust

If customers are going to trust a business with their personal data, businesses must honor that trust with the proper protections. Regulations, laws, and guidelines give customers peace of mind knowing that their information is unlikely to end up in the wrong hands.

Regulatory Compliance Helps Businesses Meet Consumer Expectations

End users expect a lot. They want personalized experiences and flawless performance — and they want it now. Regulatory compliance standards help businesses meet these expectations and secure a competitive advantage. How? By supporting data security, which then gives organizations the freedom to collect and use more data. And more data means more personalization, less friction, and better overall experiences.

Regulatory Compliance Minimizes Human Error

With firm-wide systems and processes in place, employees are less likely to make errors that result in a security breach or data loss. Even things as simple as a shared password can spell disaster for entire companies.

CHAPTER THREE:

How to Find Out Which Compliance Regulations Apply to Your Organization

Congress has enacted several regulatory statutes relating to IT compliance in response to heightened social or economic issues. The protections aim to safeguard privacy, improve IT security, and minimize the risk of fraud through the standardization of processes and enforcement of accountability.

Understanding which compliance regulations apply to your industry and organization is the first step in meeting your obligations. In the US, your business may fall under the authority of one of the following regulating bodies, among others:

- Federal Communications Commission (CC)

- Federal Trade Commission (FTC)

- Securities and Exchange Commission (SEC)

Regulations include:

- **CCPA (California Consumer Privacy Act)**

- **COPPA (Children's Online Privacy Protection Rule)**

- **FERPA (The Family Educational Rights and Privacy Act of 1974)**

- **GDPR (General Data Protection Regulation)**

- **GLBA (Gramm-Leach-Bliley Act)**

- **HIPAA (Health Insurance Portability and Accountability Act)**

- **ITAR** **(International Traffic in Arms Regulations)**

- **NERC CIP Standards** **(NERC Critical Infrastructure Protection Standards)**

- **PCI-DSS** **(Payment Card Industry Data Security Standard)**

While the above laws and standards impact the majority of businesses, the following industries are the most highly regulated:

- Financial and banking

- Healthcare

- Insurance

- Retail and e-commerce

- Utility providers

- Defense

- Government

Even if your organization does not fall under the above industries, it's still worth investigating whether you are affected by regulatory compliance. For example, any business that handles sensitive information (credit card details, Social Security numbers, etc.) must meet minimum protection standards.

The best way to find out which regulatory compliance obligations apply to your business is to do your own research. You know your business better than anyone, so read up on the above regulations.

For total peace of mind, speak with a trusted security expert. They can offer personalized advice that helps you better understand the compliance rules that apply to your operations, and what meeting those rules might look like in practice.

Who Is Responsible for Compliance?

People are necessary for ensuring compliance, with almost one in five teams spending more than eight hours each week updating policies and procedures.

The role of compliance management is evolving within organizational departments and C-suite positions. Some companies appoint full dedicated compliance teams headed by a Chief Compliance Officer (CCO). Others allocate compliance responsibilities to existing employees or outsource the duties to a third-party services provider.

Typically, a CCO is tasked with the planning and management of activities that contribute to IT compliance. This includes creating internal and external control strategies, championing a culture of compliance, and overseeing the compliance team.

"People are necessary for ensuring compliance, with almost one in five teams spending more than eight hours each week updating policies and
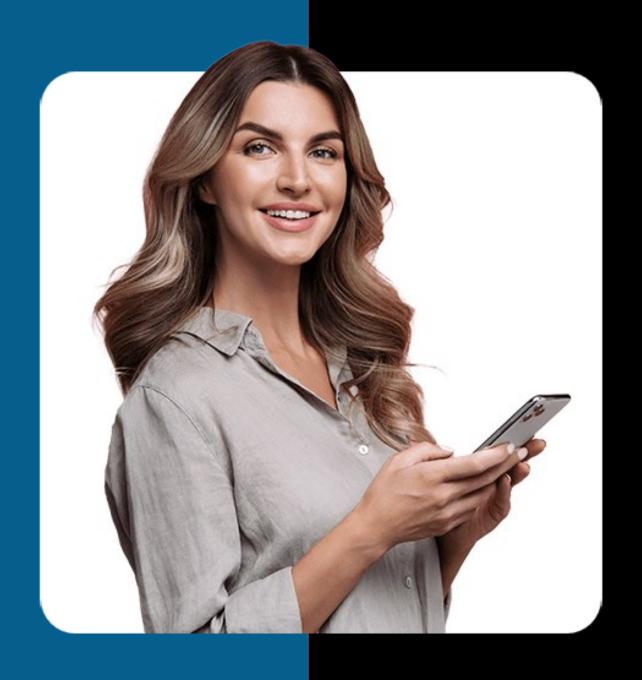
Specific duties of those responsible for regulatory compliance include:

- Identifying risk

- Designing and implementing risk controls

- Reporting on the success or failure of risk controls

- Refining control to resolve compliance issues

- Delivering advisement on regulatory compliance to the business

Training employees and stakeholders on the importance of compliance and how to uphold the appropriate protections day to day.

It is critical to recognize that, while specific compliance roles do exist within the organization, true compliance is a company-wide effort. All employees and executives are required to follow the systems and processes put in place to mitigate compliance risk and protect critical data.

What Are the Risks of Non-Compliance?

Failure to meet compliance obligations can be devastating for businesses. Here are a few things that can happen in the event of non-compliance.

Severe Penalties

Companies can be penalized in several ways for non-compliance, including fines, barriers to approval, and, in some cases, prison. Even if you are awarded a minor fine or warning without penalty, an investigation carried out by a government body into your company will cost you hours of work, legal fees, and contractor fees.

Poor Reputation

Regulatory compliance helps secure customer trust. Failure to comply can break this trust and result in severe reputational damage. Think about how you would feel if your bank mishandled your internet banking credentials or your healthcare provider allowed your records to be leaked. You'd be hesitant to do business with either again.

Delays and Limitations on Activity

Let's say you're developing a new product. You've laid the groundwork, built a prototype, refined your design, and are now ready to launch. But right at the last minute, you realize your product does not meet all compliance regulations. You're unable to go to market — it's back to the drawing board for now.

Difficulty Maintaining Staff

Talent serious about their career does not want to work for a company that has a reputation of non-compliance. If involved with a publicized breach, team members may quit or become disgruntled. People are the heart of any business, and keeping them happy is crucial to success.

Ongoing Attacks

Unfortunately, some businesses have become accustomed to large-scale security breaches that expose millions — if not billions — of records. If they are able to bounce back unscathed, they continue business as usual unaware that, for those whose records were exposed, the worst is yet to come.

Many of the most significant risks associated with security breaches resulting from non-compliance come when the data that is lost is leveraged to launch secondary attacks. Personal details are used to target individuals with malware. Ransomware, for example, can arrive in the inbox of stolen email addresses. These infected emails can appear legitimate — perhaps even from the company that experienced the initial breach.

What's more, details uncovered from a breach can be correlated with those stolen in previous attacks. For example, in one attack, the cybercriminal might learn an individual's email address, and in another, they might learn their birthday or preferred password.

In summary, the damage caused by security breaches is ongoing. Even if your business manages to recover, it's already too late for those that have had their credentials exposed.

Implementation and Best Practices of IT Compliance

There is no denying just how critical regulatory compliance is for most businesses. Now, it's time to take a look at how you can implement a compliance solution that follows best practices. We will break down the process into three distinct steps:

- The plan

- The solution

- The deployment

Let's get started.

Step 1: The Plan

When it comes to something as important as regulatory compliance, a significant amount of time and effort should be poured into the preliminary work. Planning is integral to the success of IT compliance within an organization — without it, businesses risk making critical mistakes and oversights, rendering the whole exercise a failure.

To help keep you on the right track, here are a few best practices for planning your compliance strategy:

Answer the why

Why does your business need a compliance solution? What are the driving forces, the key risks, the specific regulations that impact you and your industry? Understanding the why early in the implementation process can assist in the design and deployment of your solution.

At this early stage, it is also worth looking into the repercussion of noncompliance. We have mentioned a few here but conduct a little more research to gain a better appreciation of the gravity of the undertaking.

Identify required functionalities

What functionalities are required from your compliance solution? Come up with a comprehensive list of the types of information that you are obligated to collect and report on. For example, to meet HIPAA responsibilities, companies must track log-on attempts, so they need a solution that can collect and store events from their servers.

Here are some other functionalities to consider:
- Archiving, which allows businesses to prove compliance in the event of an audit or investigation

- Caching, which offers assurance to governing bodies that records and logs have not been misplaced or edited

- Provisioning, which automatically assigns rights to individuals and groups of users according to programmed variables

- Baselining, which enables the comparison of a specific system against other servers in the network to help measure and ensure standardization

- Real-time monitoring, which issues alerts in the event of a breach or anomaly in the system

Follow your operations from start to finish and make a note of every touchpoint. Acknowledge every time data is generated, transmitted, and accessed. Your solution must have the functionality to account for all of that data and provide adequate, compliant security protections.

Understand your environment

Determine which components of your environment are subject to compliance. For example, if you are required to trace access to secured data, you will need to monitor the computers and servers that store the information, the computers and servers used to retrieve the information, and the users that have access (and any changes to user rights).

Evaluating the technical components that play a role in your organization's compliance strategy will help you estimate the required scalability of the solution.

Calculate data volume

Before you can select a solution, it is vital to calculate the amount of data that will need to be tracked and stored. You should also identify the type of information that must be retained and the mandatory retention period.

Step 2: The Solution

Now that you have defined your requirements, it's time to select a solution. You will want to keep a few essential factors in mind when evaluating available IT compliance tools to ensure you meet your obligations.

Consider the following:

- **Supported platforms. Your compliance solution must be compatible with the full breadth of systems and environments your organization uses. Be sure that the solution you choose supports all applications that are required to be reported on in your auditing and compliance processes.**

- **Reporting capabilities. Detailed reporting that is appropriately stored is crucial in maintaining company-wide regulatory compliance.**

- **Scalability. The solution you decide on must be able to maintain efficiency even when the volume of data increases significantly. Factors like data filters, traffic compression, comparison tools, and incremental updates are all important.**

- **Security. Much of compliance is focused on safeguarding private information, which means security should be a top priority when comparing potential solutions. Look for features like traffic encryption, caching of data, guaranteed message delivery, and server/agent authentication.**

Although compliance aims to standardize processes and systems to ensure across-the-board security and protection, when it comes to deciding on a solution, there is no one-size-fits-all product.

Businesses are different. Even in the same industry and vertical, the way they operate, the culture, and the level of employee expertise are unique. It is up to you, your compliance team, or your trusted security services provider to come up with a tailored solution that caters to your one-of-a-kind requirements.

Step 3: The Deployment

You have settled on an appropriate solution that meets your organization's IT compliance needs. Now, the time has come to go live and deploy.

Keep in mind that no compliance plan is complete without comprehensive staff training. While much of regulatory compliance can be handled by either the right solution or a dedicated compliance team, it's up to each and every employee to uphold guidelines and make the right choices.

At the deployment stage, ensure all team members (including executives and key stakeholders) are on board with your compliance solution. Reiterate to them just how vital regulatory compliance is. Let them know what the risks are of non-compliance — a little scare tactic won't hurt.

Remember, companies are often held at least partially liable for employees' actions that go against regulatory guidelines and laws.

Beyond deployment

Regulatory compliance is not a set-and-forget thing. As the way we use technology evolves, legislation adapts along with it. New regulations are being introduced, and existing Acts are being modified to reflect changing user habits.

If your business is to maintain compliance long into the future, you must keep up with regulatory changes. Continuous education is not only extremely valuable but also a requirement in any compliant company. So, too, is a culture of compliance — it is not an extra step or a hassle but an integral, built-in part of all systems and processes.

Executives should lead from the top, backing compliance teams in their efforts and stressing the importance of following standardized procedures, even if they take up valuable time.

CHAPTER SIX:

How to Avoid Compliance Risks

Sometimes failures to comply with rules and guidelines are not malicious. Instead, they are honest mistakes. Where humans are involved, it is essential to account for errors, recognize the risks, and take meaningful steps toward mitigating them.

It is worth repeating — non-compliance can lead to hefty fines, barriers to market, limitations of activities, prison time, data loss, expensive legal fees, and lost customer trust.

Avoiding compliance risks should be a top priority — here are some tips to get you started.

Education

Training and education are two of the most powerful tools you have at your disposal to fight compliance risk. If employees understand their responsibilities and the consequences of failing to meet these responsibilities, they are more likely to take the correct course of action.

Invest in ongoing training. Ideally, employees should be updated anytime a significant change is made that directly impacts the business and its operations.

You can also take time during training sessions to answer staff questions and concerns. If workers are unsure of something, they should feel that they have the opportunity to make their voices heard. Processes that might be clear as day to you and your compliance team might be a point of stress and anxiety for those responsible for following them.

Encryption

If possible, enforce the encryption of data. Encrypted data cannot be access by authorized users without the correct encryption key. In the event of a breach, encrypted information is not readable by the attacker.

You can also prohibit access to certain data on devices that can't garner a secure connection. Things like public hot spots and other unsecured networks can make data vulnerable to theft.

Go for cloud storage

Modern-day cloud storage solutions are more secure than conventional inhouse servers. Ideally, your business would use both.

Cloud storage providers run data centers that are highly secure — think 24/7 security and biometrics. Not only that, they are geographically distinct from your head office, meaning if your building burns to the ground or suffers an extended power outage, your data is safe and sound.

Do not forget remote employees

It's not just the employees in your office that must maintain compliance. Your remote employees are subject, too. For some businesses, that means equipping remote workers with laptops, phones, and other necessary devices with built-in security policies and other protective mechanisms (for example, the capability to be wiped remotely).

Keeping tabs on remote team members is even more critical in light of recent events. More and more of us are working from home, which has its benefits and its drawbacks. We are using our own devices connected to our own networks to access company data.

Ignorance is no excuse, so it's vital that you take every measure possible to protect your company and its reputation.

Block unauthorized applications

Authorization mechanisms can help minimize compliance risk by preventing employees from downloading unsecure applications. These applications might not meet the minimum security standards, so they are not a viable option for your business, regardless of how useful they may be.

With the right protections in place, only approved software can be downloaded.

Defend yourself

There is no way to eliminate compliance risk entirely — especially when humans are involved. That's why it is recommended to follow strong governance frameworks and maintain defensible processes that will protect the company's best interest if an incident were to occur. Legal bills can be steep, even if the business itself is not found to be guilty.

For example, organizations can ask employees to sign off on compliance training. That way, if they fail to comply, you have hard evidence that proves they were aware of their obligations. In these instances, the company may be found to be partially liable or completely innocent, depending on the circumstances.

CHAPTER SEVEN:

Implementing a Regulatory Compliance Framework

Standardized frameworks may be used to meet best practices and adhere to regulatory requirements for IT and security compliance. These frameworks — also known as compliance programs — give companies a starting point to improve security and optimize processes to meet current and future guidelines.

Numerous compliance frameworks exist, yet many are resource-intensive to implement. Those that focus on both cybersecurity and external regulations recommend the implementation of several high-level defenses, including authentication, monitoring, reporting, encryption, risk management, and incident response. In addition, frameworks offer further guidance on employee training and engagement best practices.

Each framework approaches these elements in a distinct way. The specifics that are best suited to your organization will depend on your industry and market.

Here are some of the best and most commonly adopted compliance frameworks.

Federal Risk and Authorization Management Program (FedRAMP)

The US Federal Risk and Authorization Management Program (FedRAMP) outlines how government departments can evaluate the risks associated with cloud-based storage and infrastructure. The framework focuses on continuous monitoring to achieve real-time cybersecurity.

Control Objectives for Information Related Technology (COBIT)

The Control Objectives for Information Related Technology (COBIT) was introduced by the Information Security Audit and Control Association (ISACA) in 1996. The goal was to provide a pathway to risk reduction for organizations operating in the financial industry. The most recent rendition of the COBIT framework includes guidelines on aligning IT functions and processes to business strategy.

Consortium for IT Software Quality (CISQ)

The Consortium for IT Software Quality (CISQ) offers standards that define the automation of measuring applications' quality and size. These standards were designed to address the vulnerabilities bought to light by the Open Web Application Security Project (OWASP), the SANS Institute, and Common Weakness Enumeration (CWE). The CISQ framework is typically used to mitigate and manage risk associated with things like application security.

Privacy Shield

The Privacy Shield framework — an evolution of the US-EU Safe Harbor guidelines — was created to mitigate the risk of data tampering when transfers occur between the European Union and the United States. This is by no means a comprehensive list of compliance frameworks. Conduct your own research or reach out to a security expert to find additional frameworks that may be better suited to your business's needs.

CHAPTER EIGHT:

Own Your
Regulatory Compliance

Many businesses see regulatory compliance as a necessary evil, a whole truckload of work that takes time and funds away from growth-driving activities. In many ways, this is true. Compliance demands resources and commitment. It limits activity, permeating into every facet of your operations. It can feel like someone else has control over your business, dictating your every move, and sabotaging your aspirations.

If that rings true, it is time to shift the narrative and pivot your perspective. For businesses that use technology, regulatory compliance is not only mandatory but beneficial. Standards and guidelines take the guesswork out of security — they provide a sure-fire path to data protection and risk mitigation.

Compliance also positions your company as an industry leader, a customercentric brand that truly values the needs and concerns of others. Customers do not want to do business with organizations that are unwilling to put in the time and effort to protect their most personal, most sensitive information. And you can't blame them.

Regulatory compliance ensures companies cannot exploit consumer trust, and by maintaining compliance, you tell your customers that they are worth the effort. Because they are.

Instead of holding compliance in a negative light — own it, be proud of it. It shows you care. It shows you are human.

BLUE RADIUS CYBER
SECURITY ASSURED

Blue Radius Cyber
info@blueradius.ai

https://blueradius.ai
(512) 200-2104