Newsletter

Celebrating 31 years serving Central, N.C. *July 2021*

Best Guide to Understanding Compliance with Regulations and Standards

When you manage an organization, you hear a lot about the need to comply with HIPAA, PCI, ISO, NIST, CMMC, and many other abbreviations. But what does compliance mean? Misconceptions are common, and failure to reach and maintain compliance can lead to fines and penalties.

An article like this cannot tell you what your business needs to do to comply, but we hope to provide you with a look at the overall picture to be in a better position to understand the requirements. Feel free to contact us with questions.

Regulations and Standards

Governmental regulations are not technical documents. They rarely prescribe specific techniques. Legal experts create them for other legal experts, and regulatory boards and courts interpret them. The purpose of privacy and security regulations is to ensure that information is adequately protected and penalize those who fail to guard against misuse.

Regulations of this type are relative. They apply to both large and small organizations to guard important information and ordinary data. The greater the potential consequences of negligence are, the more the regulations demand.

Standards created by industry organizations are often incorporated into regulations. They specify in more detail what is required. Complying with industry standards helps organizations even when they are not legally required. Being certified for a certain compliance standard is a prerequisite to access some critical markets like the Department of Defense (DoD).

Achieving Compliance

Regulations and standards have organizational and technical provisions. The first step toward compliance is a determination of what requirements apply. Location and industry will affect this. A health care provider in the United States needs HIPAA compliance; a payment processor needs PCI compliance, and so on. Businesses may need to comply based on whom they deal with; for example, GDPR affects businesses outside Europe that deal with EU citizens. NIST compliance can mean many things since the agency has issued many standards that apply in different situations. The next step is to assess the environment with the applicable requirements being used as the standard.

Upcoming Events

Lunch & Learn: How Your Organization Can Survive Ransomware
July 21, 2021

Webinar: The Role Compliance Plays in Cybersecurity
July 27, 2021

For more information on our upcoming events, please visit www.tcsusa.com.

"Compliance Regulations," Continued

The assessment needs to examine physical security, policies, employee awareness, technical safeguards, and anything else that affects potential risks. A properly conducted assessment is likely to reveal areas of concern, some more serious than others. These should rank by priority and the most important ones corrected first.

In some cases, this may be enough. A well-documented set of practices, supported by evidence, may be enough to satisfy business partners and customers of compliance. The information needs to be good enough to meet an audit, so an internal assessment is enough only if people with relevant skills and experience conduct it.

Suppose the requirements are strict or the in-house expertise is limited. In that case, an organization should bring in an independent assessor to evaluate the level of compliance and identify needed remedial actions. An external assessor authorized by a standards body may offer certification if the compliance level is high enough. Many security companies provide this kind of service. It provides more robust assurance to regulators and other businesses and more internal confidence that the organization has overlooked nothing. Small organizations with a limited budget for in-house expertise can significantly benefit from outside assistance.

Staying Compliant

Being compliant requires more than a single, concerted effort that produces a document showing compliance at a point in time. Organizations are constantly changing their structure, the applications in use, and their overall technology. New risks emerge from inside and outside the firm, and this requires additional layers of security. Regulations and standards change, and you may or may not receive notice from the regulators. People become careless if they are not reminded from time to time. Without regular reviews and updates, an organization will eventually drift out of compliance. We would suggest this is a semi-annual need, but some certifications may require renewal on a more frequent basis.

Scheduled reassessments will help identify any areas where compliance needs boosting. It will make sure that the organization is fully prepared to protect its information and demonstrate up-to-date compliance if an auditor comes calling.

Any organization that deals with sensitive information needs to comply with relevant standards and even regulations. Failure to do this can hurt your business's reputation and lead to penalties.

5 Ways to Protect Your Company's Information

Recently, I was talking to someone in our office about the problems that come with using older versions of Office. He automatically mentioned that various employees using different versions under a single network can make it difficult to make a complete update on everyone's computer at once. Then, I questioned if there were security issues with having older versions of Office. He had completely forgotten that you are more vulnerable from doing this.

Sometimes we forget that there are simple ways to keep our data safe, such as protecting your company's information by using the newest version of Office.

For those of you that don't know, safeguarding in the IT world means -- being proactive against attacks, threats, and disasters that may cause a business' or organization's data to become defenseless. Keeping data secure is a lot easier now that there are multiple ways to take precaution.

Automated Backups

There are a variety of backup methods including the use of a backup system, a data support center, Cloud-based backups, and more. All methods have their pros and cons, but the decision should be based on what is cost-effective and efficient for your company.

Considering most people do not choose the first house they see or the first car they test drive, your decision to choose a possibly expensive data backup prevention method should not be any different. Therefore, it is best to do your research first.

Install a Firewall and Filters

Coming from someone who has had to deal with the same continuous pop-up message about my expired free trial of protection services too many times to count, I can understand the irritation when it comes to dishing out money for something that is keeping you safe invisibly. I always question: would it make a difference? I know the answer, and you do too. That is why firewalls are necessary. Hardware firewalls are the best because they keep a protective barrier between the internet and your business' data.

Besides firewalls, other important safety measures include anti-virus protection, as well as spam and content filters. These three data support methods keep your incoming and outgoing information secure.

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

Protect Mobile Devices

All devices with sensitive information, including smartphones, laptops, and tablets have the capability of being attacked. If you are like me, you might use your phone's hotspot to get an Internet connection on your laptop. Sometimes when I am finished using my laptop, I will forget to turn off my hotspot, which turns something that is very convenient for me, into something very convenient for the local hacker that wants to get into my personal information. Hotspots and public Wi-Fi are breeding grounds for data loss by an elusive cybercriminal.

So, next time you are thinking about using a work computer in a public place, make sure you have end-to-end encryption on your laptop and a secure password with diverse characters, numbers, and letter case.

Pick a Quality Vendor

Just like finding the best data backup method takes time, so choosing a quality provider or data support center. Over half of all companies that lose data are out of business within six months, so a third party vendor must be well equipped to handle their client's needs. It might be best to talk to a few different support centers and ask valuable questions to make sure they are certified and have an optimum experience to help your company in case of a disaster.

Make a Disaster Recovery Plan

One of the most tedious things to do is make a disaster recovery plan and keep everyone up to date with its procedures. However, this will help your company in the long run when systems are working smoothly after coming into work one morning to an in-house server failure.

Some of the most important things to remember about a disaster recovery plan are: perform an audit, disseminate information, and practice your plan.

Safeguard Business Data Today

Most small to medium-sized businesses want to put sales and customer service before IT prevention; however, that can be detrimental to a company. Safeguarding is all about being proactive.

TCS webinar

The Role Compliance Plays in Cybersecurity

Date: Tuesday, July 27th
Time: 11:00 AM ET
Presenter: *Barry Utesch, President, TCS*
Registration: Visit tcsusa.com/events/ or call 336.804.8449

Compliance is not just for regulated industries anymore. Requiring standardized compliance and security is on the horizon for all businesses. Most executives are aware of compliance, but it is often difficult to understand and even harder to accomplish.

Organizations are constantly changing their structure, applications, and overall technology. New threat risks are continually emerging from inside and outside the business requiring additional layers of cybersecurity. Protecting confidentiality, integrity, and the availability of data is crucial for your company. Failure to do this can hurt your business's reputation and lead to loss of business.

Key Takeaways

- Understanding Compliance
- General Guidelines for Standards and Regulations
- Maintaining Compliance in Your Organization

Attend this webinar and understand how an improved security posture for compliance can help elevate your business above the competition.

On-Demand Webinar: Achieving Data Backup at Microsoft O365 Cloud

Most organizations do a great job moving their data to the cloud, but no one asks these crucial questions, "What is the backup strategy in the cloud, and why is it important?" Companies assume the cloud provider has the sole responsibility of protecting and backing up data. Driving factors for managing data are legal recovery, HR issues, cyber threats, and compliance.

Watch this webinar to gain insight on why a backup strategy in the cloud is essential.

Visit landingpages.tcsusa.com/webinars to watch this and other webinars available on-demand.

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

totalcomputersolutions

How Your Organization Can Survive Ransomware

Join us for our upcoming Lunch & Learn!

Date: Wednesday, July 21st
Time: 11:45 AM ET
Cost: Free
Location: Undecurrent Restaurant, 327 Battleground Ave., Greensboro, NC 27401
Registration: Visit tcsusa.com/events/ or call 336.804.8449

Ransomware is the most dangerous trend in the business world today. Organizations are losing time, data, and money due to these malicious attacks. Over 300 million Ransomware attacks in 2020, and 90% of companies are not prepared to respond. Learn how to increase your knowledge of Ransomware origins, strategies and how to react to these alarming cyberthreats. Understanding the anatomy of an attack will help you survive it.

Key Topics for Discussion

- Best Ways to Protect Against Ransomware
- Its Happend! What to Do Next
- Response Strategies After An Attack