Beyond "Check the Box" Compliance: Finding Compliance Utopia

Before we get into the specifics of finding compliance utopia, let's look at what compliance really is and why we should care about it. Ultimately, compliance is adherence to a standard or a particular set of rules, recommendations, or guidelines.

WHY DO WE CARE?

Standardization is important for several reasons. First, it allows us to increase capacity or efficiency in our workflows, which should directly impact the bottom line. When standardization exists, it can be measured and improved. Second, it improves the experience of the organization's customers. Standardization allows us to more easily identify the bottlenecks and pain points in order to improve upon our processes. Third, it indicates a mature organization, which can help build market value. Finally, and most importantly, standardization is most often created to protect information, people, or both. Organizations rely on their data being available and secure.

Standardization and compliance are key to protecting the availability, confidentiality, and integrity of a company's services and information through a systematic process approach.

Standardization and compliance are key to protecting the availability, confidentiality, and integrity of a company's services and information through a systematic process approach. A poorly implemented compliance program will often lead to an information security breach or human harm.

One such example was a cancer center out of the University of Texas that compromised the data of over 33,000 patients from one unencrypted laptop and two unencrypted thumb drives. An investigation found that policies were not updated and followed. The organization suffered a 4.3 million dollar loss from the event. Additionally, in one of the largest breaches on record, the insurance organization Anthem compromised the passwords and private information of 79 million individuals by failing to implement appropriate security measures. Both of these organizations had undertaken compliance initiatives; however, they proved ineffective. It is simply not enough to have a compliance program, it is important to have effective compliance.

It is simply not enough to have a compliance program, it is important to have effective compliance.

Now that we know what compliance is and why it is important, we need to understand why compliance programs routinely fail the companies that work to implement them. One common misconception, frequently used to roadblock successful compliance, is that it's too expensive. As a result, companies choose to ignore the requirements and run the risk that they are not caught in a breach or system failure. While it's true that compliance can be costly, there is a wide gap between costs that are truly necessary and what compliance can end up costing.

"Check the box" compliance is more dangerous than doing nothing at all–it provides a false sense of security that prevents real vulnerabilities from being identified and addressed.

Another hindrance to successful compliance is "check the box" compliance. This approach to compliance only focuses on fulfilling minimum requirements of the standard, without consideration to the scope of application, or to the effectiveness of the solution. The end result of this approach is wasted time and money, as true compliance is not achieved, and information or individuals are left exposed to risk. Some would argue that "check the box" compliance is more dangerous than doing nothing at all–it provides a false sense of security that prevents real vulnerabilities from being identified and addressed. Successful compliance is often thwarted by trying to use "compliance in a box" toolkit solutions. Many great software tools and applications provide compliance support solutions. A comprehensive compliance program cannot be purchased in the form of a toolkit. While these tools may be useful to speed up compliance program implementation, they cannot replace the knowledge and understanding gained through following the process. Effective, successful compliance is a process and is not as hard as most people assume.

So, what does it take to achieve simple, cost-effective, successful compliance? The process involves three major phases: 1. Developing Requirements 2. Performing Risk Assessment; and 3. Applying Solutions. Figure 1, below, shows how each of the phases interlock and rely upon each other for a fully functioning compliance program.

Figure 1: The Compliance Process

Let's look at each phase and what is involved.

REQUIREMENTS

The most common mistake in aligning with a standard is not having complete knowledge of the standard within the organization. It takes some time to read and digest the standard and fully understand what is required versus recommended or advised; however, the time investment will be well worth the reward. As a side note, summarized information in a whitepaper or in a table isn't good enough. Someone within the organization must be an appointed subject matter expert. This designated person (or persons, preferably) should be someone at a level who can implement change. Consultative support can be very useful, however, it should not be used to absolve the organization of its responsibility to be informed. Additionally, this subject matter expert will serve a useful purpose by acting to check and balance proposed solutions. As an employee of the organization, they should always have the company's best interests in mind.

Consultative support can be very useful, however, it should not be used to absolve the organization of its responsibility to be informed.

RISK EVALUATION

The next phase in the process is risk evaluation. This phase is the most important part of a compliance program and includes several important steps. Figure 2 shows a graphical representation of the risk assessment process, including the risk evaluation phase and the solution identification phase.

Figure 2: Risk Assessment Process

APPLIED SOLUTIONS

Now that the organization's risks have been identified, what's the next step? Risk can be mitigated, transferred to another entity, or even accepted, in some cases. This is an area where most organizations struggle because they don't have a good understanding of the total risk picture. Repeatedly, we've seen expensive solutions implemented to address a vulnerability, but because the entire risk picture is unclear, the value of the solution is not fully recognized.

By knowing the requirements, what needs to be protected, and the associated risks, a clear picture is presented that will lead to a cost-effective solution.

One important factor to remember in this part of the process: there are many ways to protect information and adhere to requirements. A little research can go a long way. Ask colleagues what solutions they employ and what challenges they have experienced. Build a relationship with a trusted advisor in that particular area of expertise. Often, simple solutions are overlooked. This is where knowing the requirements of the standard is crucial. By knowing the requirements, what needs to be protected, and the associated risks, a clear picture is presented that will lead to a cost-effective solution. It should not be assumed that the most expensive solution is the best solution. Implementing a cost-effective solution can be straightforward. Invest in understanding the whole picture before implementing compliance solutions. The reward will be a better understanding of the organization, making it more stable and better protected.

SUMMARY

For some, compliance is a dirty word. It means spending lots of money and time. For others, it is ambiguous and intangible. It can't be clear, straightforward, or quantified. These assumptions surrounding compliance can be overcome by taking a systematic approach to implementing a process. Compliance is an industry in and of itself as there are companies whose sole purpose is dedicated to helping organizations meet those standards. However, regardless of each company's individual budget, the important takeaway is that compliance doesn't need to be complicated, overly burdensome, or costly. Focusing on a clear understanding of the requirements, taking the time to get a complete picture of the risk, and evaluating all possible options is the best way to find compliance utopia; compliance that serves its purpose is cost-effective and makes the organization better.

MARY KNOTTS
Partner at
PEAKE Technology Partners

ABOUT THE AUTHOR

Mary Knotts is a Partner at PEAKE Technology Partners and focuses on IT operations, as well as Governance, Risk, and Compliance for PEAKE and its clients.

Mary received her MBA from the University of Baltimore and is a Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), and Certified Information Systems Auditor (CISA).

Mary also leads PEAKE's Security Risk Assessment (SRA) team, which helps healthcare clients identify and mitigate information security risk and ensure compliance to HIPAA and other standards.

PEAKE™
TECHNOLOGY PARTNERS