Realtime
publishers

Implementation Strategies for Fulfilling and Maintaining IT Compliance

Kevin Beaver

sponsored by

QUEST SOFTWARE®

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: Understanding the Real-World Issues Associated with IT Compliance

Compliance is often thought of as a dirty word. Rightly so—businesses are struggling more and more with the compliance requirements being pushed on them from every angle. There are numerous state, federal, and international compliance regulations affecting businesses around the globe:

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Gramm-Leach Bliley Act (GLBA)
- US state breach notification laws
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union (EU) Data Protection Directive
- Hong Kong's Personal Data (Privacy) Ordinance
- Japan's Personal Information Protection Act (JPIPA)

Much to the chagrin of business leaders, these regulations aren't going away. The good news is that gaining and maintaining control of IT compliance doesn't have to be all that difficult. If done correctly, compliance can actually serve as a business enabler and help minimize information risks long term. The key is to understand what compliance is really about and how its many parts can be managed effectively throughout the business.

Applying the Compliance Big Picture to the Business

Compliance is the adherence to a set of rules or laws that some governing body thinks is the best fit for your industry and your business if you are somehow handling sensitive consumer information—aka personally-identifiable information (PII)—or sensitive financial reporting information. Compliance has evolved over the years as a result of businesses not doing what they probably should've been doing all along.

There's a fiduciary responsibility to protect PII and financial reporting information, but what about your own data? If you're running a business and doing the right things to keep your information systems protected, intellectual property likely comprises a significant portion of your information. I often see companies focusing on one area but not the other. Oftentimes, PII gets all the attention while intellectual property is ignored. Still, in other cases, intellectual property is taken seriously but PII is simply ignored.

In essence, compliance represents forced business changes in the name of information privacy and security. Businesses are being held to a higher standard now because things have changed in this era. Since the advent of the PC, the Internet, and mobile computing devices, most businesses rely on some form of electronic information. These technologies and associated ways of doing businesses have introduced enormous risks that no business had to endure just a few decades ago.

Another issue driving compliance is the general expectation of privacy and security. Individuals themselves aren't necessarily demanding that their personal information be protected. However, there are various organizations, associations, lobbyists, and so on representing the public as a whole. These bodies are aware of the issues and are driving compliance in IT. These requirements have manifested themselves through the legislative process, and we've reached a point where we have high expectations to keep sensitive information protected.

To many people, compliance is black and white, on or off. This is especially true for the legislators who write the laws and regulators who enforce them. There's a general belief that everyone simply needs to comply with X, Y, or Z regulation and everything will be good. The reality is that nothing is this simple. There's a disconnect, especially with some of the early information privacy and security regulations such as SOX and HIPAA. These regulations are more vague and often don't include key guidance that is provided in more recent legislation.

Although there is a set of general information security best practices, regulatory agencies such as the Federal Trade Commission (FTC) and Department of Health and Human Services (HHS) often consider the topic black and white. Their approach is "Every business just needs to do these things." Regardless of whether the requirements are based on logic or information risk and whether the requirements are enforceable or have basis in reality, the fact is that the exist and regulated businesses have to comply.

Note

PCI DSS is different from the government regulations in that businesses have come together to develop a set of security requirements for other businesses. Although it's a bit more explicit and streamlined than government regulations, that doesn't necessarily make PCI DSS compliance any easier.

This approach to compliance often extends to the audit function as well. Interestingly, certain internal and external auditors I've worked with see compliance as black and white—something that must be done regardless of any risk, logic, or reasoning. On the flip side, I've seen auditors who don't take compliance seriously at all. They see it as thorns in their sides and an impediment to doing business—someone else's problem. Dealing with their own internal audit issues, many auditors are not pleased with having to adhere to yet more regulations. Rightly so, as compliance often creates a large burden on internal audit teams not to mention the expenses associated with implementing the proper controls required to bring the information systems environment into compliance.

Note

There's a tight relationship between compliance and the audit function. An audit compares what you're supposed to be doing with what's actually being done based on best practices, generally-accepted standards, and/or compliance regulations.

One of most critical aspects of compliance is seeing the big picture and ensuring that all of your systems are working together towards a common goal. You might claim that your business is compliant because you have certain policies, contracts, training, and so on in place, but true compliance is much more than that. Compliance is about having the right operational, technical, and people controls in place working together in a culture that supports the goals of the business.

Furthermore, compliance is about visibility, control, and automation. Whether you're a Microsoft shop running Active Directory (AD), SharePoint, and Exchange; a UNIX/Linux-only shop; or a mixed-technology environment, there are numerous tools available to ensure compliance, including tools for identity and access management, systems monitoring, and disk encryption and data loss prevention (DLP) on the endpoint side and intrusion prevention and advanced firewalling on the network perimeter.

Tip

From analyzing overall information risk to controlling who has access to what on the network to finding security vulnerabilities on a periodic and consistent basis, you *have* to have good tools. Without the proper tools, there's no reasonable way to keep things in check.

If you use the right technologies, have the proper business processes in place, and address security issues at a high enough level, you're going to be able to tackle the compliance issues you're faced with much more effectively and efficiently. The intended outcomes of a long-term compliance strategy are about adhering to security standards and minimizing business risk. This will ensure that the sensitive information you're processing and storing—PII and intellectual property alike—stays protected.

Another benefit of compliance is that it can be seen as a competitive differentiator and business enabler. I have many clients that use me to help ensure their networks and Web applications are secure and meet the necessary compliance requirements. Most of the well-known regulations require periodic security assessments.

When you're proactive in this way, you'll be ready to answer the tough questions when your business partners and customers ask "How do we know your systems are secure?" By using the right technologies and processes, you can hand over your latest reports to show where things currently stand rather than waiting for someone else to tell you and getting caught off guard. Marketing and sales teams can—and should—use this information and positioning to the business' advantage. Savvy people working for business partners and prospective clients will see this and know that you take security and compliance seriously.

Tip

Practically every aspect of a business can benefit from a well-planned and executed compliance strategy. Are the right people in touch with compliance in your organization and singing its praises? Spreading the word can be a wonderful business development tool.

Integrating Compliance as a Way of Doing Business

Many people see compliance as a barrier that they must adhere to because someone (that is, a government bureaucrat) is making them do it. However, compliance can become second nature—yet another aspect of the business—if it's properly integrated into the culture and business processes at a high level.

For compliance to work well, it requires management support and visibility across the organization; it is also necessary for the right people (compliance officers, IT directors, and network administrators) to keep management in the loop and the conversation going regarding compliance. A solid security committee can help pull this together and ensure accountability and responsibility across all levels of the organization.

Making compliance an ordinary part of the business also requires a shift in mindset and culture related to what's at risk and how business gets done. Culture changes are brought about by management. That's why it's so critical for management to realize what's at stake and what security and compliance truly mean to the business.

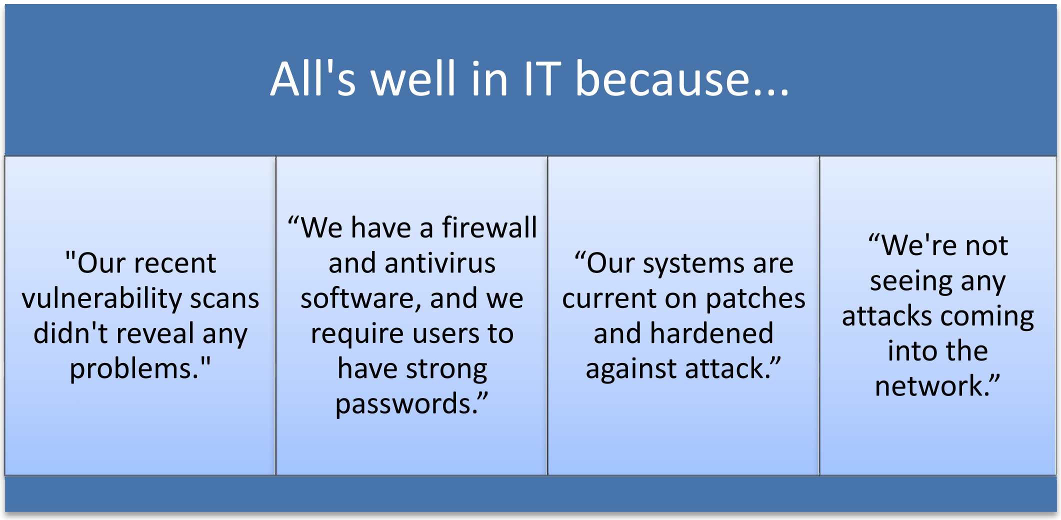
You can claim to have all the policies and fancy technologies in the world, but talk is cheap when it comes to compliance. Many people I interview during my security assessments are out of the loop regarding security and compliance. They simply don't know what's expected of them. Improperly set expectations—or lack of expectations altogether—can be found in practically every IT failure, compliance gaffe, and data breach. That's why it's absolutely critical to have everyone on board with the long-term goals of the business with awareness of how each person can help achieve those goals in their work.

Simply put, IT compliance can be a threat or an enabler. Looking at it from the perspective of overbearing government regulation, compliance clearly creates barriers to getting things done. But it doesn't have to be this way if it's done properly—that is, if reasonable controls are put in place that provide good visibility into your network environment and help set everyone up for success. Again, management buy-in and support is essential. Everyone needs to know what's expected of them.

In the end, compliance doesn't have to cripple the business, and it won't if you manage your compliance initiatives at a high enough level. By approaching it from an information risk management perspective, you'll be able to address the requirements of HIPAA, HITECH Act, SOX, GLBA, PCI DSS, and so on across the board. In other words, by not managing each and every regulation in its own silo, compliance will simply result from your higher-level information risk management efforts.

Questioning What's Really Happening on the Network

Network administrators are at the core of security and compliance. However, in certain cases, the situation of fox guarding the henhouse arises. So much trust is placed in the IT team that there's often very little accountability. The assumption is that all's well because the people in IT said it is—but that's a dangerous approach. For this reason, people working in management, compliance, and on change control committees undoubtedly hear excuses like those illustrated in Figure 1.1.



All's well in IT because...

"Our recent vulnerability scans didn't reveal any problems."

"We have a firewall and antivirus software, and we require users to have strong passwords."

"Our systems are current on patches and hardened against attack."

"We're not seeing any attacks coming into the network."

Figure 1.1: Common quotes regarding the state of IT.

Why is it this way? Well, I've been in these situations and it's tough. In most cases, the reality is that people in IT are doing the best with what they've got. Rather than working on more strategic and analytic issues that impact the business long term, many folks in IT work in a reactive mode continually putting out fires. Much of this can be attributed to the lack of time. There are simply not enough hours in the day for many network administrators. However, on the flip side, it can be argued that certain people in IT may not be making the best use of their time; IT, security, and compliance suffer as a result.

Another contributing factor is the lack of good tools. Many network administrators are forced to make do with what they've got, which, in many cases, is little to nothing. Security and compliance require visibility, control, and automation—none of which can exist without the right tools to ensure the information systems environment is kept in check.

Additionally, many IT professionals have trouble seeing the big picture. To certain people, IT is all about bits, bytes, and command prompts. They often fail to take the business into account. Much of this attitude comes from the top down through management not properly setting expectations and holding people accountable for the business' bottom line.

> **Note**
>
> People aren't born with time management and goal setting skills. When people don't realize how important such skills are for working in IT, security, and compliance, the business ultimately suffers.

The lack of long-term perspective and communication breakdowns between management and IT often create a disconnect between the parties and on throughout other parts of the organization. The cycle continues.

So what can be done about this problem? As previously mentioned, management buy-in for security and compliance initiatives is a must. In order to accomplish this, both groups of people have to realize it's a two-way street. Management needs to understand that IT, security, and compliance are crucial to the business. Likewise, IT staff members need to understand that they're there in support of the overall business objectives. Once the ball gets rolling, IT staff members need to keep management informed and in the loop. These two factors feed off one another in a continual cycle of leadership and personal responsibility. Eventually, a solid culture of information risk management can evolve.

Once vision and lines of communication are established, it's important for both management and IT staff to ask the right questions for further clarification. This puts the concept of "trust but verify" into action and helps ensure that everyone's on the same page with good information.

So how should managers approach IT staff regarding these issues? Simply put the ball in their court. Empathize with the complexity of the network environment and the fact that managing the security of it all must be difficult. Then ask what you can do to help make their jobs easier so that they can ensure the network is secure and the business has reached a reasonable state of compliance. Specific questions to ask include:

- Are we keeping logs of Internet usage?
- How are we tracking the addition and deletion of user accounts?
- Can I see the network activity report from the past week/month/quarter? What trends are you seeing?
- Can I see the latest security assessment report? Have we addressed all the issues that came up in the last report?
- What are we doing to monitor and ensure system performance and uptime? Do we have a plan for when critical systems go down?
- Have you taken an inventory of the sensitive information we process and store? Have you determined where it's located on the network?
- Are we up to date on software patches on our workstations? Servers? Databases?
- Have we addressed the issue of laptop and mobile storage encryption? What can we do to decrease the odds of a data breach in the event of loss or theft?
- What security controls are in place for personally-owned smartphones and tablet computers?
- Is there anything that can be done to improve our visibility into what's taking place on the network to help minimize risks?

If you're a network administrator, it's critical to realize that everything you do should be in terms of the business. Tie everything you can back to the business where possible. Talk about how security and compliance issues are impacting other organizations in your industry. In particular, talk about what's happening on the network right now and how it's impacting the business. Present what's going to happen if you don't do X, Y, or Z in terms of security and compliance.

> **Tip**
>
> Security and compliance are ultimately management's responsibility. Network administrators and others working in IT shouldn't be afraid to ask management what's expected of them. This can be a good way to create and maintain visibility for security and compliance projects long term.

In the end, every choice you make in IT either moves the business *toward* better security and enhanced compliance or *away* from better security and enhanced compliance.

Do You Need to Look in Every Nook and Cranny of the Network to See What's Going On?

It's common for network administrators to keep their fingers on the pulse of the visible issues, but it's often the little things that get you. Believing that compliance gaps and security breaches will be highly visible is a common and dangerous oversight. Some common network security and compliance oversights to consider include:

- Failure to keep security policies, and more importantly, security plans and procedures updated. The documentation side of IT security and compliance is no doubt boring, but it's arguably one of the most important pieces.
- Weak Windows domain and standalone system passwords. One weak password is all it takes to compromise an email account, establish a VPN connection into the network, or decrypt data that was assumed to be secure. You wouldn't believe how often this issue comes up.
- Inconsistent patching of workstations and especially servers and database systems. Anything with an IP address is fair game, and there are free tools available that make exploitation of common vulnerabilities quick and easy.
- Assuming that technical controls are enough. They're not. You have to strike a balance with technology and business process. Those two combined with periodic and consistent user training are crucial to minimizing information risks.

Focusing on the urgent and important systems and issues at hand is essential. Go for the low-hanging fruit—the quick-fix gaps and vulnerabilities that will provide you the most bang for your buck. That's where your network is bleeding the most and where the greatest business risks originate.

Don't fret—you don't have to drain the ocean all at once. Simply getting started now and building things out as you move forward can pay off before you know it.

Understanding Everyone's Unique Issues and Concerns

Quite often, the goals and requirements of one part of the business work against the goals and requirements of other parts of the business. This juxtaposition often shines through clearly when talking about IT, security, and compliance as Figure 1.2 shows.

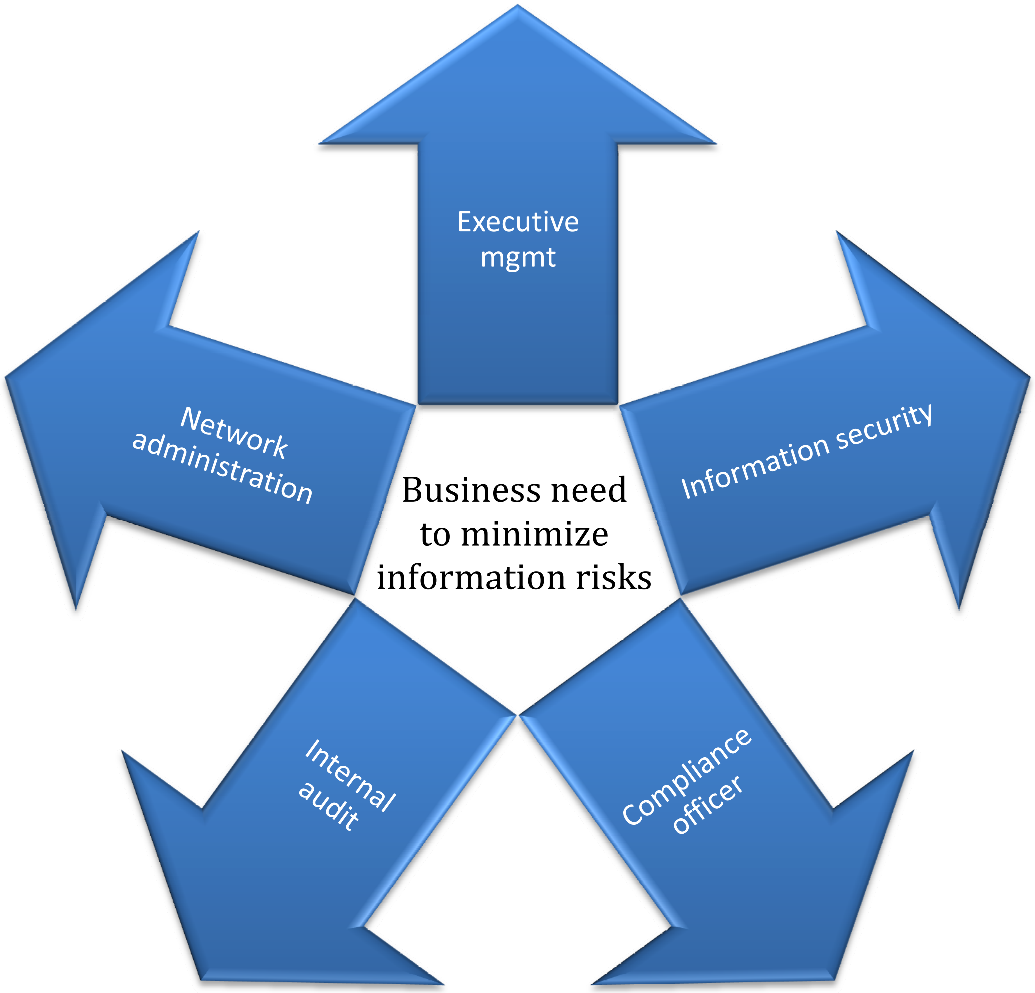


Figure 1.2: Unique stakeholders often have differing views on information risk management.

Management has a unique set of needs and so do internal auditors and compliance managers—likewise with information security staff and network administrators. In many situations, it's as if the needs of each group responsible for security and compliance are completely undermining everyone else's efforts.

Looking at businesses as a whole, any given commercial business that intends to stay afloat must do two things: acquire and keep customers. This ongoing process requires minimizing expenses and maximizing profits—something that IT is at the heart of. Management has to answer to its shareholders and stakeholders when questions arise related to either expenses or profits, and IT is often the first to be shoved to the back of the budget priority list. Government agencies, schools and universities, and non-profits are a bit different. However, these organizations still have to work within the confines of a budget.

Note

Regardless of the business type, IT, security, and compliance are often seen as an impediment to moving ahead while, at the same time, the business couldn't survive without its computers and applications.

Additionally, management is being questioned more and more on security and compliance issues. Questions such as: How are you handling this? What systems do you have in place for that? Middle management needs to be able to provide good information to upper management when these types of questions come up. The list of questions and the list of people asking the questions are endless, but there is a silver lining. The situation is bringing more and more visibility to IT and compliance, which is usually a good thing.

An important idea for business managers to remember is that it's okay to have security and compliance gaps. Many people I've met are concerned about having a flawless environment where everything's in check and no information risks exist. They essentially want a clean audit report. Unfortunately, such a scenario doesn't exist in reality. Given the complexity of any given network, there's simply no way to ensure that everything is locked down 100 percent. If it were, the odds are good that no one could get anything done.

Tip

By striking a good balance between information risk management, convenience, and usability you can please management and keep them on your good side.

Looking beyond management, and depending on the size of the organization, internal audit and compliance staff members have their own approaches to security and compliance. In essence, internal audit is concerned with the inner checks and balances in and around IT to ensure things are in line. My experience has been that internal auditors aren't concerned as much with the letter of the law as they are with ensuring a specific set of IT controls are in place and internal policies are being adhered to. Compliance officers, however, tend to know HIPAA, HITECH, PCI DSS, and other regulations and will do what it takes (sometimes to the detriment of the business) to ensure IT is meeting all of the documented requirements. Overall, internal audit and compliance staff want answers to questions such as those highlighted in Figure 1.3.

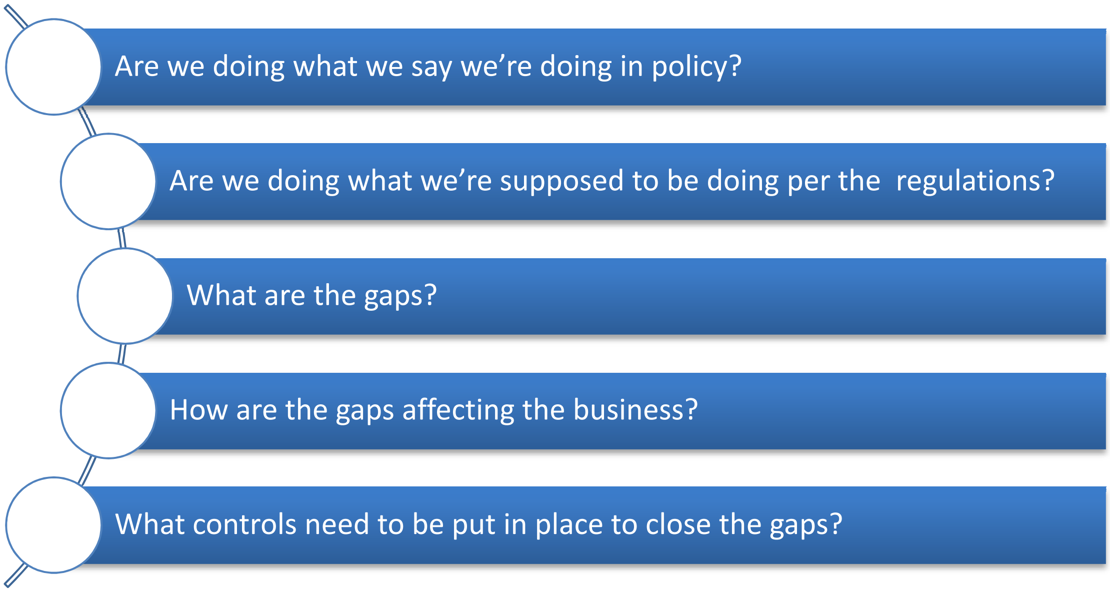
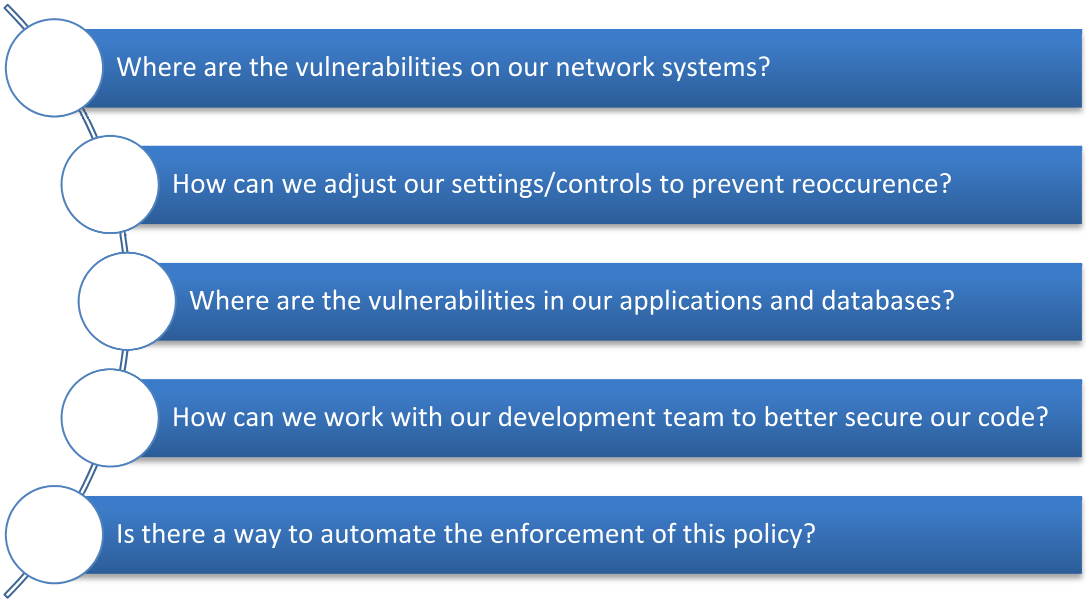

Are we doing what we say we're doing in policy?
Are we doing what we're supposed to be doing per the regulations?
What are the gaps?
How are the gaps affecting the business?
What controls need to be put in place to close the gaps?

Figure 1.3: A sampling of internal audit and compliance staff concerns.

It's important to differentiate *what you're doing in policy* and *what you're supposed to be doing per the regulations* because they're often two completely different issues. Gaps often exist and, in many cases, politics, culture, and technical issues drive needs more than anything else—and the cycle of non-compliance continues.

There's also the information security team. From managers to administrators, information security staff members often have their own unique set of issues and goals that impact the bottom line of security and compliance. These may or may not be the same people responsible for IT management and administration depending on the size of the organization, but they have the same goal: knowing at any given point how secure the environment is. Information security staff members want answers to questions such as those illustrated in Figure 1.4.



Where are the vulnerabilities on our network systems?

How can we adjust our settings/controls to prevent reoccurence?

Where are the vulnerabilities in our applications and databases?

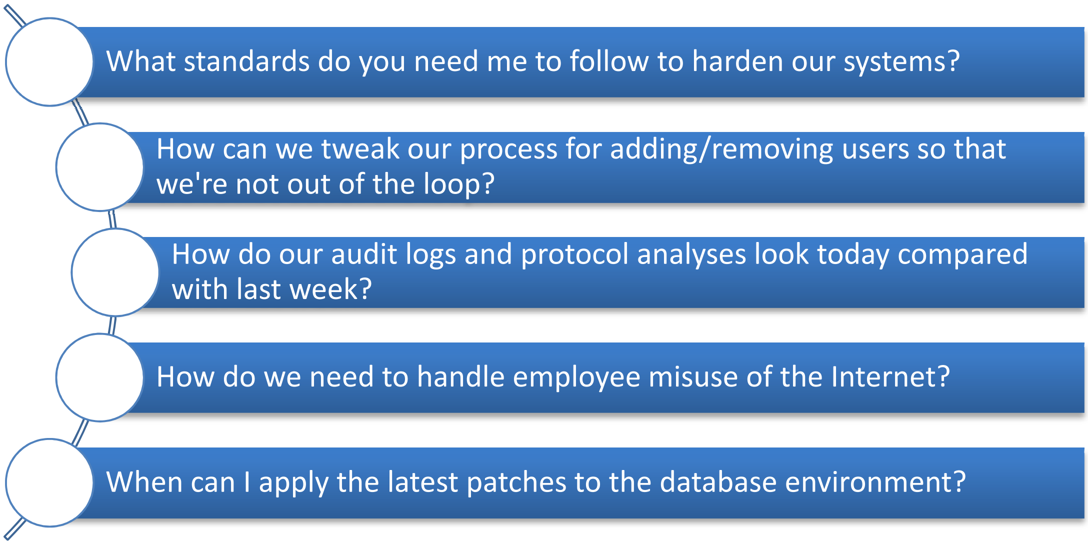
How can we work with our development team to better secure our code?

Is there a way to automate the enforcement of this policy?

Figure 1.4: A sampling of information security staff concerns.

Generally speaking, the information security team mantra is to get things secured and compliance will soon follow. Overall, the goal is to establish a cohesive set of higher-level controls that will address most of the compliance requirements, then tweak things as needed moving forward.

Network administrators and other general IT staff are a bit different. They want answers to more granular questions such as those Figure 1.5 show.



What standards do you need me to follow to harden our systems?

How can we tweak our process for adding/removing users so that we're not out of the loop?

How do our audit logs and protocol analyses look today compared with last week?

How do we need to handle employee misuse of the Internet?

When can I apply the latest patches to the database environment?

Figure 1.5: A sampling of network administrator and general IT staff concerns.

Network administrators have a unique set of issues to deal with. They're sort of the last layer that helps the rubber meet the road when it comes to security and compliance. Management expects the computer systems to be up and running, internal audit and compliance are continually questioning their work, and information security is there to ensure things stay in check.

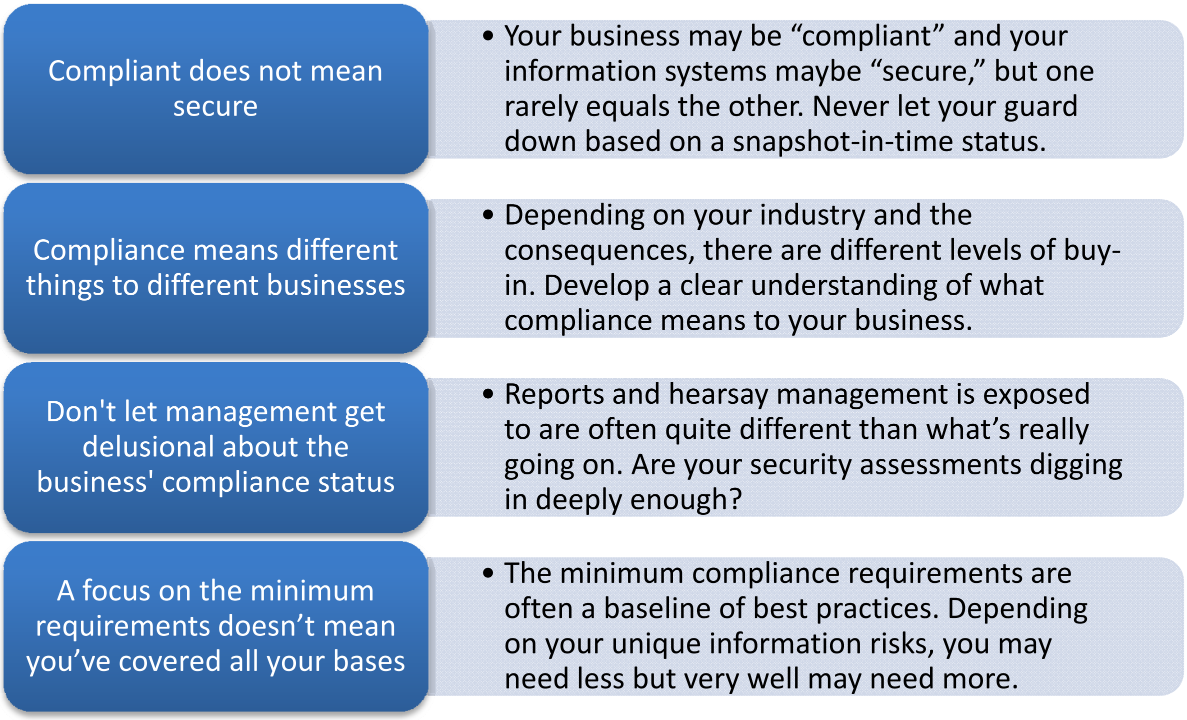
One of the greatest burdens that network administrators have to deal with is the number of compliance regulations. Not just the regulations themselves but the little nuances of each one that so many people expect to be implemented properly. These compliance requirements are all over the map, and it's often the network administrator that has to sort through and figure out what's needed where. Given the additional layers of security and compliance oversight, it really shouldn't be this way. Again, trust but verify and let each person in each particular role do their fair share to ensure things are in check.

> **Warning**
>
> Security and compliance are not IT-centric problems. They're *business* issues that need to be dealt with at the appropriate levels. IT staff should be utilized for input and implementation of the technical pieces along the way.

As you can see, every role in the security/compliance equation has a unique focus. From higher-level business issues all the way down to system configurations, there is a variety of tasks that make up an overall IT compliance program. Just make sure each role is carrying its weight.

Common Assumptions and Oversights About Compliance

As you move forward with your compliance initiatives, it's important not to get caught up in the numerous misconceptions that often arise. Figure 1.6 outlines common compliance assumptions and oversights you should be aware of.



Compliant does not mean secure

- Your business may be “compliant” and your information systems maybe “secure,” but one rarely equals the other. Never let your guard down based on a snapshot-in-time status.

Compliance means different things to different businesses

- Depending on your industry and the consequences, there are different levels of buy-in. Develop a clear understanding of what compliance means to your business.

Don't let management get delusional about the business' compliance status

- Reports and hearsay management is exposed to are often quite different than what’s really going on. Are your security assessments digging in deeply enough?

A focus on the minimum requirements doesn’t mean you’ve covered all your bases

- The minimum compliance requirements are often a baseline of best practices. Depending on your unique information risks, you may need less but very well may need more.

Figure 1.6: Compliance misconceptions you need to avoid.

There’s a saying that experience is something you get just after you need it. It’s important to educate yourself and stay on top of your security and compliance initiatives so that you don’t get bitten in the first place. Preparation, open-mindedness, and consistency over time can help tremendously toward your security and compliance—and ultimately information risk management—programs moving forward.

Compliance Case Study

YYZ Bank and Trust is a large regional bank providing traditional and online banking services. For years, YYZ Bank’s CIO, Mike, and its VP of Internal Audit, Matt, were under the impression that their network administrator Joe had things under control. Even their newly-hired compliance manager, Chris, was fairly impressed with the level of effort the bank had put forth to comply with the Gramm-Leach Bliley Act (GLBA) and PCI DSS. After all, Joe had been with the bank for over a decade and knew every single system like the back of his hand. Joe had even gone so far as writing his own internal intrusion prevention system (IPS) from scratch.

Any time a user tried to access the core processing systems of the bank, an unrecognized computer connected to the network, or external vulnerability scans were detected, the IPS would immediately cut off network access. The IPS worked so well that many thought Joe had missed his calling by not starting up his own business designing and selling his IPS appliance.

Unfortunately, Joe's IPS combined with the stringent network access controls he had built into his network switches got in the way of employees doing business—a lot! If anyone needed to do to anything on the network out of the ordinary, they had to go see Joe and ask for permission.

Although many people at the bank were disenchanted with the stringent network controls Joe had in place, everyone including Mike and Matt felt comfortable that the bank's sensitive information was locked down. When asked by management if everything was secure, Joe would quickly reply "Of course!" No one bothered to confirm or verify his statements. Well, as Mike and Matt would soon find out, "locked down" is a relative term. As with many things compliance-related, what often appears to be whiz-bang security technology is often just a front to cover up bad business processes and poorly-run systems underneath.

Mike and Matt decided to hire a third-party information security expert to perform an independent security assessment of their environment. What they learned in the final deliverables of this assessment project was eye-opening. They found out, among other things:

- Nearly half of their servers and 25% of their workstations weren't current on operating system (OS) and third-party patches leading to vulnerabilities that could be exploited to gain full access to the systems by an insider using free and simple tools.
- None of the bank's database servers had been patched in more than 7 years—many of which had default user names and passwords.
- Users had been sharing out their local hard drives to everyone on the network, exposing spreadsheets, PDF files, and more containing PII.
- Their online banking system's authentication mechanism was easily manipulated, allowing an attacker to bypass the login process and gain access to the backend data.
- A lack of communication between HR and IT created serious user provisioning gaps that led to dozens of former employee user accounts remaining enabled and accessible via the bank's VPN.

Interestingly, Joe's IPS would have never detected or blocked any such breaches. The reality is that there's no way to know for sure whether any breaches had occurred to this point. Joe's IPS may have kept certain parts of the network locked down but not all of them. This is a classic case of a network administrator protecting all the wrong things and management being too trusting of their employees and assuming all's well in IT.

Coming Up in the Next Chapter

With this exposure to the essence of compliance, we're ready to dig a bit deeper. Chapter 2 covers compliance cost considerations. In particular, how to be smart with your security and compliance investments and why it doesn't have to be all that expensive.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.