realtimepublishers.com™

The Shortcut Guide™ To

Network Compliance and Security

AlterPoint

Don Jones

Introduction to Realtimepublishers

By Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical technology topics—at no cost to the reader. Although this feat might sound somewhat impossible to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading is the equivalent of any similar printed book you might find at your local bookstore—with the notable exception that it won't cost you $30 to $80. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions and the release of a new edition possible in a far shorter timeframe than is the case with conventional printed books. Because Realtimepublishers publishes our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create "dream team" projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at http://www.realtimepublishers.com, or calling us at 707-539-5280.

Thanks for reading, and enjoy!

Sean Daily
Founder & CTO
Realtimepublishers.com, Inc.

Foreword

In this new age of regulatory compliance, we are finally experiencing a rush to improved process discipline based on configuration and change management. This development is most welcome—the need for discipline has never been more apparent. Although shining examples of organizations that run with a high degree of structure exist—this guide offers practical guidelines that characterize such operations—they are rare. For the majority of organizations, structure is weak or missing. This situation is changing because it must if those organizations want to survive and thrive in an environment of unprecedented challenges.

As one investigates configuration and change management processes and technology solutions, it is apparent that the field as a whole is currently in its earlier stages of evolution. Solutions now focus on a specific technology domain (for example, network, software distribution, patch management), but consolidation is in rapid progression. New technology always has a narrower focus because the initial technical hurdles are narrow. These hurdles are now being overcome by pioneering vendors in the configuration and change management market. The next stage in the market's evolution is consolidation across vendors, technology domains, and process breadth. This stage is now beginning.

This consolidation is inevitable and necessary, but it is important to understand the unique characteristics and business implications inherent in each domain. The network is a perfect example to illustrate this need. IT services are end-to-end phenomena. There are many components involved in every service and there is an intricate network of relationships between these components.

Networking has become so pervasive in IT environments that we often forget about the underlying complexity resident in this interwoven labyrinth of technologies. Although many are familiar with the fundamentals of networks, precious few truly comprehend the internal details of networking technology. Even many so-called network engineers often know only a fragment of the reality that exists under their watchful eyes. Networking vendors have succeeded at hiding much of the complexity through mass-production, miniaturization, and software. This simplification has been a hallmark of successful technology; however, it has its limits. In the case of networking, the complexity must still be controlled by someone with the right tools. Attempting the same control without such tools is becoming not only inefficient but nearly impossible.

The right tools, in the hands of a skilled practitioner, offer a means to both understand and control the behavior of a complex system. In the case of networking, no tool category promises more value than effective network configuration and change management solutions. The network configuration and change management market is gaining momentum because networking represents a domain that has received little attention when it comes to structured operations. This neglect is ironic because network infrastructure has been a major driving force of the IT revolution for more than 20 years. Because networking is so critical, however, we tend to rely more on an elite class of subject matter experts for support instead of turning to structured processes and automation technologies.

The trend toward processes and automation does not suggest that network configuration and change management threatens network experts with extinction, though. Quite the contrary is true. As a result of exploding complexity, professionals with the necessary skills are becoming scarce and are therefore becoming expensive. Any organization that wants to operate its network with fiscal responsibility is forced to augment a small team of experts with technologies that automate some of the tactical aspects of this work and enable less-skilled, less-expensive staff to perform other tasks. The experts should be reserved for more advanced work to more effectively leverage resources. The experts benefit because the technologies assist them in their goal to develop future capabilities to best serve business requirements.

Senior business and IT leaders recognize the role of the network as the central nervous system of the operation. With such heavy reliance on this infrastructure, leaders know that they must manage the risk associated with this critical business asset. The most prominent risks today are compliance and security; new methods and technologies are in demand to minimize this risk because traditional methods are failing. In response to this demand, automation and structured processes yield discipline, and discipline reduces risk and saves costs. Thus, there is a critical need for all of IT, especially the network, to institute discipline in the entire network life cycle.

The need for discipline in the network is reflected in network configuration and change management. When we have more accurate configuration information, we can more effectively fulfill compliance requirements, enhance security, better assess the impact of changes, improve the automated root cause analysis of performance problems and failures, and optimize the planning for business change. The enhanced visibility of the structure and behavior of the network has endless benefits. To maintain consistency in this vital information, a strong change management process must be in place and enforced. Even a seemingly benign circumvention of the change process can render the configuration data nearly useless. Automation technologies offer a means to enforce compliance to the change process, speed execution of changes, minimize errors in the process, and ensure that changes are authorized.

As we enter the next chapter of IT evolution, we are faced with the mandate for better discipline and better efficiency. Both are required virtues if we want to transform IT from a “necessary evil” to a valued business enabler. Senior leaders demand better alignment of IT and business goals and systems. Configuration and change management, especially in the networking domain, offers a means to accelerate our quest toward this ideal.

To remain relevant and even prosper in this new world, we must embrace the concepts presented in this guide. The skills needed for the future lie not so much in the infrastructure technologies themselves but in the ability to apply and control these technologies to enhance the performance of the business and to minimize risk to the business. Note that the business is the common theme. Although this transition in focus might be difficult for many of us who rode the technology wave to success, it is a fact. It is now time to join the new revolution or be left behind.

Glenn O’Donnell
Program Director
META Group, Inc.

Copyright Statement

Chapter 1: Understanding IT Compliance

Compliance has become one of the hottest buzzwords of the information technology (IT) industry. With new legislation—such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, 21 Code of Federal Regulations (CFR), and more—compliance has become the most important item on many IT professionals' to-do lists. Compliance has gained the spotlight and has therefore become a much more recognizable issue at higher levels of management, which means that is it is now being given more attention throughout many organizations. The quest for compliance has launched entire consulting practices, resulted in the development of products, and become the focus of billions of dollars' in technology spending. But what *is* compliance?

This guide explores the underlying meaning of IT compliance, apart from all the hype and publicity. It will explain how the IT industry has been handling compliance for decades, and how new technologies and techniques can help you better handle compliance moving forward. To prove that compliance has always been with us, we'll focus on an often-overlooked area of IT—the network infrastructure.

What is Compliance?

Having worked in the IT arena for quite some time, it's fun to see all the media focus on compliance, all the compliance-specific projects being implemented in organizations across the world (particularly in the United States), and the general buzz about compliance. A few years ago, we simply called it "following the rules."

Defining Rules

Until fairly recently, companies more or less were able to define the rules of IT conduct within their organizations. For example, they might decide that only members of the Human Resources (HR) department would have access to employee salary information, or they might write a policy stating that employees aren't allowed to test the company's internal security measures without written permission. Rules defined the answers to questions such as: Who was allowed to have keys to the filing cabinets? And Who was allowed to come into work late and who wasn't? Those rules were the beginning of the more formal idea of compliance in application today, and they've been around since long before computers came on the business scene.

However, that is not to say that companies have been subject to only their own rules. For example, United States Department of Defense (DoD) contractors have always been subject to externally developed rules regarding the confidentiality of information, rules for performing background checks on potential employees, and so forth. By following these externally developed rules, the contractors helped ensure future business with the DoD. In other words, they were worried about *compliance* in order to maintain their businesses.

Today, several external agencies—primarily government legislators—have gotten into the act of writing business rules. These rules tend to target specific types of industries—such as health care, financial services, and so forth—and, rather than focusing on day-to-day business issues, these new sets of rules tend to concentrate on protecting the personal information that these businesses handle (for example, customer data, health care records, financial information, and so forth). These external rules are *no different* from the business rules that have been created and applied within organizations from the beginning. True, the new rules give organizations less control because the rules are externally developed rules and are enforced through legislation, but *complying* with those rules is the same activity that it always has been.

Meeting Rules

So what is compliance? According to Dictionary.com:

> **com•pli•ance** *n.* The act of complying with a wish, request, or demand; acquiescence.
> *The American Heritage Dictionary of the English Language, Fourth Edition*

Compliance, then, is simply the act or process of meeting rules. It doesn't matter from where those rules originate, and it doesn't really matter what *kind* of rules they are—business rules, legislation, security rules, and so forth—simply meeting them means that you're in compliance. Thus, the first crucial idea that you should bear in mind throughout the rest of this guide: *Compliance is simply the act or process of meeting rules, no matter who made the rules or what the rules apply to.* You'll find that compliance—especially with regard to your network infrastructure—makes more sense, and is easier to plan for, if you think about *all* of your business rules in one big lump.

True, failing to comply with an externally developed rule might carry a heftier financial penalty than failing to comply with an internally developed rule. However, presumably your internally developed rules are just as important for other reasons, such as profitability, governance, and so forth. The second crucial idea to consider throughout this guide: *Meeting rules isn't sufficient.*

Enforcing Rules

Suppose that your organization has adopted a rule that requires all computers to be behind at least one, if not two, firewalls so that no computer has a direct connection to the Internet. This rule is a simple enough business rule and is fairly common in most organizations—so common, in fact, that it is often not even written down.

Suppose that you sit down and look at your network configuration one day, and it looks like the diagram that Figure 1.1 shows.

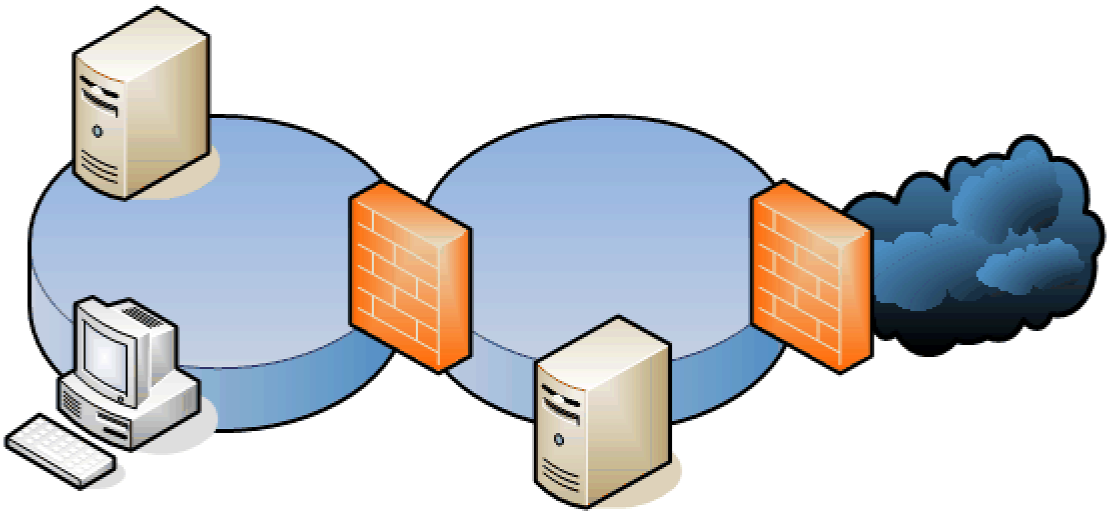

Figure 1.1: Sample network diagram.

Is your network compliant? It appears to be; every computer is behind at least one firewall, and most are behind two. Is it safe to fire off a positive report to the stockholders, letting them know that the network's security is meeting the company's policies? Absolutely not.

Rules are made for reasons. Your company's policy regarding firewalls wasn't put in place to help sell firewall hardware; it was put in place to protect company assets—the underlying assumption being that un-firewalled computers aren't safe.

Looking at the network diagram, you can see that all computers are protected by at least one firewall—*today*. What about yesterday? What about tomorrow? What about 10 minutes from now? Network configurations can change drastically in a few *seconds*, so your point-in-time audit of the network configuration is practically useless for ensuring compliance.

To illustrate this point, consider note passing in class when you were a kid. Some kids could pass notes all the time and never get caught, but notes were still being passed. The teachers' point-in-time audits simply failed to catch the activity. In other words, from the teacher's point of view, the class was compliant with all note-passing regulations, but the class was anything but. There was no *enforcement*.

In the years that I have been working in IT, I have primarily run across companies that use auditing—point-in-time inspections of their environments—to maintain compliance with whatever rules they faced. Today, with compliance becoming a more serious issue for many industries (especially compliance with legislation such as HIPAA, Sarbanes-Oxley, and so forth), many companies still rely on point-in-time auditing to ensure that they are in compliance. Although auditing definitely has a useful function—visual inspections at a specific point in time are important to maintaining any set of policies, they should be considered only a *part* of your overall compliance plan; a plan should include some kind of *enforcement* technology.

For example, if someone was mispronouncing your name in a conversation or meeting, what would you do?

1. Correct them.
2. Ignore them half of the time and write a report about the mispronunciation the other half of the time.

Choice number two is auditing; choice number one is enforcement. Auditing catches *some* problems *some* of the time; enforcement *corrects* problems as soon as they occur. Enforcement is an automatic reaction to error, bringing the enforced entity back into line. At the very least, enforcement can be implemented as a kind of continuous, automated auditing, where out-of-compliance conditions are automatically detected and reported, allowing a human being to take corrective actions.

Let's get back to the childhood classroom for another example: Suppose your teacher installed motion detectors that would sound an alarm every time notes were passed between students. Although the teacher would likely continue point-in-time audits—turning away from the blackboard every few minutes to visually scan the classroom—enforcement would be provided by the motion detectors. Sneaky Billy in the next row would always get caught because the enforcement system would always be on the job.

Next, consider your network infrastructure for an enforcement example. Your organization probably has rules about what traffic is allowed in and out of the corporate Internet firewall. Let's say that you only allow HTTP traffic into a perimeter network so that your Web servers are accessible to the public, as Figure 1.2 illustrates.

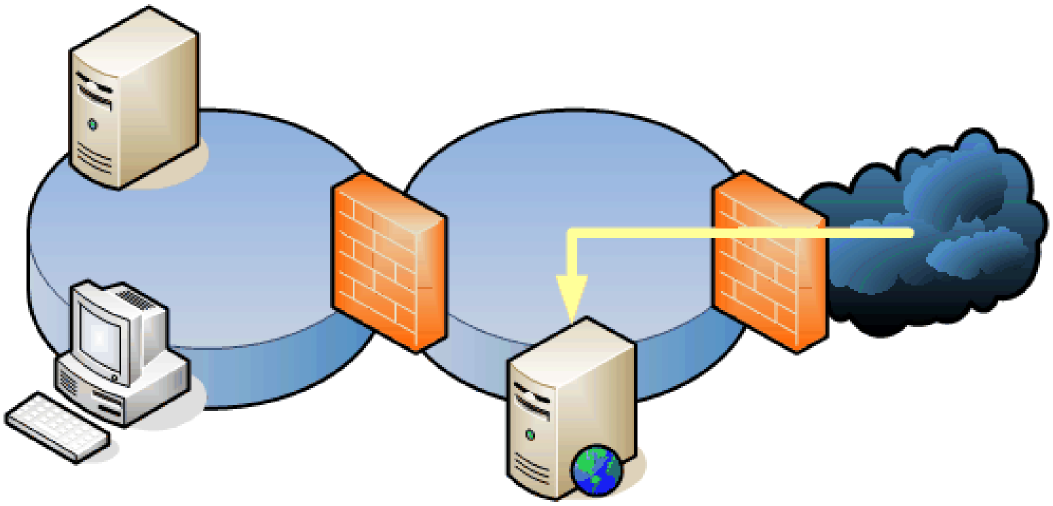

Figure 1.2: HTTP traffic is allowed to reach a Web server.

Now suppose that a firewall administrator makes a one-time exception so that his computer can also receive file-sharing traffic. His favorite band has a new MP3 out and he wants to share it with the world. As Figure 1.3 shows, the firewall configuration is now out of compliance with company policy.

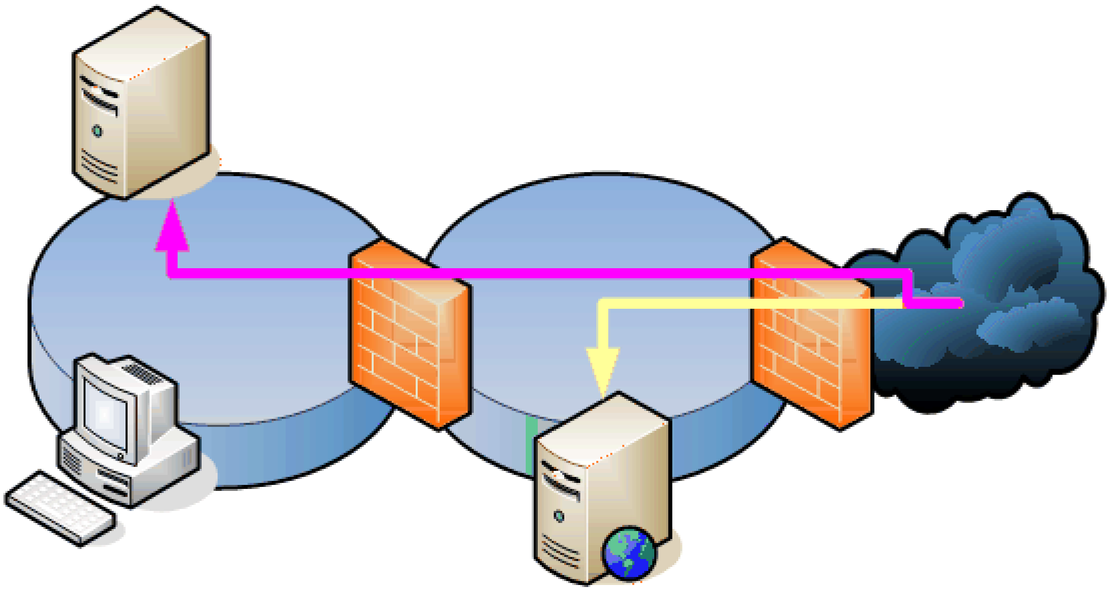

Figure 1.3: The firewall now allows additional traffic through to the intranet.

An audit of the firewall's configuration might not catch this problem because the firewall administrator knows when and where audits occur and can remove the offending configuration before then. However, an enforcement solution would immediately detect the change to the firewall's configuration, realize that the change was out of compliance with company policy, and at the very, least alert someone—or several people—to the problem. A well-designed enforcement solution might even be able to roll back the firewall's configuration to a known-compliant version, effectively undoing the improper change.

Why bother with enforcement? You must develop the right attitude about compliance, if you haven't done so. Even legally mandated rules have a higher purpose than merely fining you if you aren't compliant; rules are designed to improve business, protect businesses and customers, and more. Auditing might be sufficient to keep the legislators happy, but it won't help serve the rules' higher purpose: To protect and improve your business. Enforcement, however, serves the rules' spirit, rather than its letter, by ensuring that you remain compliant at all times.

Verifiable Compliance

I’ve worked with a few clients who have developed comprehensive policies for how their network infrastructure should work, and spent tens of thousands of dollars configuring the network to meet those policies. But simply *doing* so doesn’t tell you that you’re compliant. And, while they had some great process flowcharts that described how various key processes would work, having those in place doesn’t tell you that you’re compliant either.

Doing vs. Being

In the compliance world, you’re not compliant until someone looks at your environment and says that you are. Whatever processes or systems you’ve got in place don’t matter; the rule of the road is that only an audit can determine whether your organization is compliant. I know—I just got through saying that auditing doesn’t prove anything. Unfortunately, the general world of compliance—particularly when it comes to legislative compliance—doesn’t understand anything beyond mere auditing. Look at it this way: Auditing serves the *letter* of the law, while enforcement serves, as I said earlier, its *spirit*.

Let’s go back to the classroom for an example. Suppose the school has a no-note-passing policy, and teachers are responsible for policy compliance within their classrooms. Your teacher puts in the motion detector I mentioned earlier, and makes periodic scans of the classroom to make sure that there is no funny business going on with the kids in the back row. Is the classroom compliant?

Not technically. Everything is in place to support compliance, but the teacher can’t be certified as compliant until an outside auditor peeks in and checks everything. Are there, in fact, notes being passed? If not, then the classroom is compliant; if a note changes hands, then the classroom isn’t compliant, and the teacher has a meeting with the principal that afternoon. Figure 1.4 helps to illustrate the difference between the policy and reality in network infrastructure terms: The policies are in place for a firewall, but one isn’t being utilized.

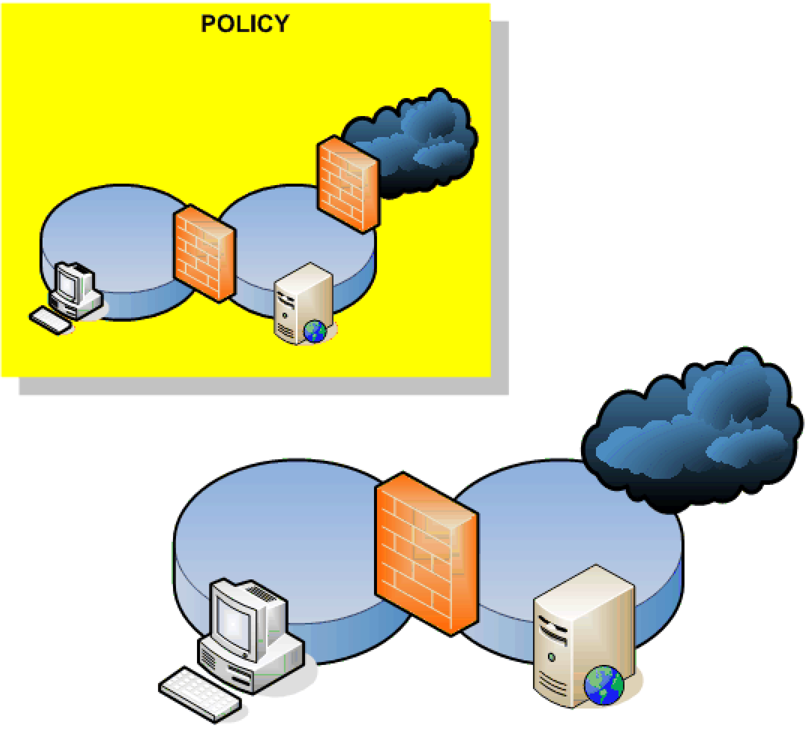

Figure 1.4: When the policy doesn't match reality, you're not in compliance after all.

A good auditor only checks the *end state* for compliance: The rule says no note-passing, so the auditor checks to see whether notes are being passed. The actual *means* of compliance aren't a concern because it doesn't matter how compliance is achieved, only that it is, in fact, achieved.

In the IT industry, of course, testing the end state can be a complex, challenging, and technical task. For example, how do you test the end state for a policy that says that only HTTP traffic can be allowed into the network? You must conduct a test in which you try to get other forms of traffic in. Unfortunately, most auditors don't have the technical background necessary to conduct this type of end-state audit. Instead, they must rely on auditing your measures: They'll check the firewall configuration against a template, and if the configuration doesn't match their template, then there is a compliance issue.

The downside to auditing measures—as opposed to auditing end state—is that the technology for doing so is complex. Simply because some measures are in place to implement a policy doesn't mean that the policy is fully implemented. It's possible, for example, for a firewall's configuration to meet the requirements of the auditor's template while still allowing traffic that the firewall shouldn't. Had the auditor tested the end state rather than just looking at the firewall configuration, it would be obvious that something was letting illegal traffic into the network. It's the difference between *doing* and *being*: Implementing (and checking) your measures are the *doing*, but it doesn't guarantee compliance. *Being* compliant means testing for compliance to the rule, whatever it is, and not worrying about how the rule is being implemented.

Auditing vs. Enforcement

The difference between auditing and enforcement remains important. Because testing the end-state of IT—especially network configurations—can be so complex, organizations are often forced to rely on configurations to ensure compliance. In other words, it's often impractical to test a firewall to make sure it's completely compliant with company policies, so you must rely on carefully crafted configurations to ensure that the firewall will behave as desired. Given this limitation, enforcement of the proper configuration—rather than simply conducting point-in-time audits—is absolutely critical. The smallest change to a firewall configuration can result in an out-of-compliance situation; because you're not able to readily test new configurations for end-state compliance with policy, you instead need to catch those changes—even the smallest ones—and deal with them appropriately.

Back to the classroom for an example: Suppose the school doesn't have any auditors who can look to make sure that note-passing isn't taking place. Instead, the school comes up with a standard classroom configuration—motion detector and periodic visual scans by the teacher—to remain compliant with the policy. Given that the end-state will not be tested—that is to say, nobody will be actually watching to make sure that note-passing doesn't occur—the school is relying entirely on its configuration—motion detectors and visual scanning—to comply with the no-note-passing policy.

Simple point-in-time auditing would have the principal stopping into each classroom once a day and making sure that the motion detectors are turned on. But if the principal sticks to a schedule, teachers will know to flip the equipment on at the proper time of day. In other words, the principal's spot checks are useless for ensuring compliance because they don't tell him that the configuration is proper *outside* of the spot-check times. This example illustrates the basic failure of auditing that was described earlier.

Enforcement, then, would require the motion detectors to alert the front office whenever they were turned off. Because the school is relying on the proper configuration to maintain compliance, this notification feature would help the school ensure that the configuration is in place at all times. Removing the motion detectors' power switch and hardwiring them to a power source is another possible enforcement technique, helping to ensure that the configuration can't be modified. However, some form of feedback from the motion detectors would be required so that the school could ensure that power wires weren't cut, motion detectors weren't blocked, and so forth. In other words, if you're relying entirely on your configuration to ensure compliance, you need an enforcement mechanism to ensure—*guarantee*—that the desired configuration remains in place.

> **en•force** *tr.v.* (1) To compel observance of, or obedience to: *enforce a law.* (2) To impose (a kind of behavior, for example): *enforce military discipline.* (3) To give force to; reinforce.
> *The American Heritage Dictionary of the English Language, Fourth Edition*

The crucial idea: Enforcement *compels* observance of your policies; it *imposes* your policies rather than simply prescribing them or monitoring them. Enforcement, then, is the key to compliance in the IT industry.

Compliance and the Law

As we explored, compliance has always been with us. Every time an employee is sent home to change into more appropriate workplace clothing, compliance is being maintained. Compliance is simply meeting a set of rules, whether those rules relate to dress code, business practices, or security practices. What has become so important in today's IT environment is compliance with legislation: External rules that literally carry the weight of law, and which, if not *enforced* within an organization, can also carry significant legal and financial consequences.

HIPAA

HIPAA is "summarized" in a 289-page tome available from the United States Department of Health and Human Services. Essentially, HIPAA boils down to two broad sets of rules governing how anyone involved in the health care industry must conduct business. The portability section of the act defines certain standards for health coverage to be moved between carriers; the accountability portions of the act—the ones that everyone's thinking about when they say "compliance" in most cases—define rules for the handling, storage, and disclosure of patient information. For example, HIPAA outlines strict guidelines for which personnel inside an organization can access patient information.

The implications of HIPAA for an organization's network infrastructure are obvious: Your network provides access to much of this information. Ensuring that your network has been configured to support security will make HIPAA compliance and enforcement more practical. Ensuring that your proper network configuration is being *enforced* will help prevent costly fines that result from accidental or even malicious reconfiguration.

The Sarbanes-Oxley Act

Although the Sarbanes-Oxley Act of 2002 imposes several new regulatory controls for financial services firms—primarily public accountants, the compliance issues surrounding this legislation pretty much boil down to accountability and recordkeeping. In other words, firms must maintain pretty tight security over their records, must be able to provide a report of who can and has accessed those records, and must maintain those records for specified periods of time. For example, Title VIII of the act defines the knowing destruction of documents to impede, obstruct, or influence a federal investigation as a felony.

Does this legislation have any bearing on IT and, more specifically, network infrastructure? Broadly speaking, the Sarbanes-Oxley Act requires the ability to audit and control the availability of information, and your network infrastructure is one of the most common means by which information will be made available. Section 404 of SOX contains guidelines about annual reports that state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, an assessment of those procedures' effectiveness, and so forth. In other words, you need to know how people are accessing your information, *prove* you know it, and issue a report evaluating your effectiveness.

The act doesn't lay down a lot of rules for exactly how you're supposed to accomplish compliance, but best practices have been developed in the industry: Rely on centralized control and management of all resources to the greatest degree possible. If your company has 10 firewalls, managing them independently will result in inconsistent coverage and will make reporting on their effectiveness more difficult; centrally controlling them from one place makes reporting and configuration easy.

Another important consideration: Do you even *know* about all your network infrastructure devices? You're required to control them all, but companies almost always forget about a switch, hub, or router or two, especially in large networks. Tools that can automatically discover devices as well as bring them into compliance (or at least alert you to out-of-compliance conditions) are valuable assistants in maintaining compliance with the Sarbanes-Oxley Act.

21 CFR

Targeting United States federal agencies (and in many cases their civilian contractors), 21 CFR creates criteria for electronic recordkeeping. 21 CFR is primarily focused on the pharmaceutical and other Food and Drug Administration (FDA)-controlled industries, outlining requirements for electronic records, electronic signatures, non-repudiation, authenticity, and other controls.

The effects on your network infrastructure are obvious: Data must be transmitted securely and must not be modified in transit. Data must be protected. Quite simply, your network infrastructure—the basis for all electronic traffic and security—must be configured to facilitate data protection, and it must remain properly configured at all times. Again, *enforcement* becomes more important than mere auditing, because a momentary lapse in security—one an audit might not catch—can result in data modification or other actions that would result in non-compliance with this legislation.

Other Laws

In addition to HIPAA, the Sarbanes-Oxley Act, and 21 CFR, there are many other laws that might affect IT processes in your organization. The following list highlights some additional legislation to consider:

- The Children's Online Privacy Protection Act (COPPA)—Mandates that Internet sites obtain and maintain parental permission to use, collect, and retain children's personal information. Even for family-oriented sites that make special "safe areas" for children, this legislation places HIPAA-like burdens for maintaining data and confidentiality.
- The United States' Electronic Signatures in Global and National Commerce Act (E-Sign)—Gives the same legal weight to electronic signatures and documents as physical ones have. Recordkeeping and security becomes critical; although E-Sign doesn't mandate accounting or recordkeeping, the legal weight this legislation gives to electronic documents makes it in every organization's best interests to develop strict policies regarding e-document control.

- The United States' Government Information Security Reform Act (GISRA, which is part of the Defense Authorization Act of 2001)—Requires agencies to implement electronic information security measures to assess their security management practices, and much more. Controlled by the Office of Management and Budget (OMB), this legislation has penalties for failing to comply such as total de-funding of all IT efforts within the non-compliant organization.
- The Gramm-Leach-Bliley Act—Requires financial institutions to safeguard their clients' private information. Broader in scope than the Sarbanes-Oxley Act (which primarily governs the activities and standards of accounting firms), the Gramm-Leach-Bliley Act applies to any financial services organization and imposes HIPAA-like standards for protecting customers' information.
- The European Union (EU) Data Protection Directive and Electronic Signature Directive—Implements E-Sign and Gramm-Leach-Bliley Act–like regulations for companies and organizations operating within the EU. The Data Protection Directive in particular governs the use of personal information within the EU and requires both strict controls and comprehensive accountability.

These pieces of legislation all have a common thread: They require your network infrastructure to be tightly configured and controlled. Your network infrastructure forms the basis for all IT security, protecting your network from unauthorized access and helping to protect information in transit between computers. *Enforcing* a secure infrastructure configuration is crucial to maintaining compliance with these pieces of legislation.

Compliance and Security

Here's what Dictionary.com has to say, in part, about security:

> **se•cu•ri•ty** *n.* Something that gives or assures safety, such as…measures adopted, by a business or homeowner, to prevent a crime such as burglary or assault.
> *The American Heritage Dictionary of the English Language, Fourth Edition*

Preventing burglary sounds like a pretty common business practice. Retailers usually require employees to lock the doors when closing the store, which is a simple, common-sense business rule that is nonetheless written down as policy in any retailer's employee handbook or operations guide. Thus, security is just a rule or policy that safeguards the business' assets in some fashion.

So why is such a big deal made over security? Companies spend thousands of dollars on security audits of their IT systems, when they rarely spend as much time and effort auditing, for example, the use of their company logo in marketing materials. Yet you can make a very good argument that misuse of a company logo can have just as devastating an impact on the business as data theft. I'm not trying at all to understate the importance of security: I'm simply pointing out that security is just another set of business rules that must be somehow enforced. Many solutions and methodologies designed for general business policy compliance are also effective security tools, simply because security is just another set of business policies.

The phrase *security compliance* can be used to refer to the subset of your rules that deal specifically with security issues; however, always keep in mind that security is something that, in general, you should deal with along with all your other business rules, not as a separate entity.

Common Security Compliance

It's useful to quickly review the types of security compliance issues that commonly arise in an organization, particularly with regard to the network infrastructure. After all, the network itself isn't as simple or as straightforward as just setting up permissions and auditing on a file server, making network infrastructure security compliance somewhat more of a gray area in many people's minds:

- Permissions—Typically, organizations are concerned about who has the ability to modify the network infrastructure, specifically the configurations of routers, firewalls, and so forth. These components' configurations are your network infrastructure and represent the basis for the network's security.
- Reliability—Organizations are often concerned about disaster recovery and reliability: If a devices becomes misconfigured, how quickly can the misconfiguration be identified and the device reconfigured properly? One weakness implied by this question, of course, is that management is reactive. A better question is how can device misconfiguration be automatically prevented or how can the proper configuration be automatically enforced?
- Auditing—Even when authorized changes are made to a device, organizations typically need to understand who made the change and when they made it. Such is definitely the case for unauthorized or incorrect changes.
- Standards—As I've said before, auditing the end-state of anything technological can be difficult, so organizations instead tend to rely on a set of configuration standards that implement a desired level of functionality and security. Such being the case, a common compliance issue is ensuring that those standards are met. Organizations typically do so through sometimes-cumbersome manual reviews by peers and committees; in fact, this very review process is a part of most industry best practices, including the Information Technology Information Library (ITIL) standards.

These are the four major categories that the network infrastructure most often presents in terms of compliance. In addition to relating to the network's stability and reliability, these issues all directly relate to the security of the network in a fundamental sense.

Rolling Security into Overall Compliance

There are some easy steps for rolling security into your overall compliance plan. The primary technique is to eliminate everything that refers specifically to electronic security. Instead, rewrite policies to simply cover *information* security, regardless of whether that information is printed, spoken, or electronic. If information is sensitive or confidential, it remains so no matter what medium it exists in; if you're planning to secure your company's file servers, lock the filing cabinets, too. If you're going to require encryption for data transmitted across the Internet, ask yourself why you wouldn't do the same for data transmitted across FedEx or a fax machine.

Security is just another set of rules. Incorporate your security policies into the rest of your business policies for availability, recoverability, business practices, and so forth. In the end, security concerns have an effect on nearly every area of your business, so dealing with security as a standalone subject makes no practical sense.

Security on its Own

One of the reasons against considering security as a standalone set of issues is that security's needs and goals are actually contradictory to most businesses' needs and goals. For example, a *completely secure* business would have no Internet connectivity, no windows, no phone lines, no fax machines, and so on. Such a business would be virtually guaranteed that confidential information would never leave the company—and such a business could be virtually assured of rapid bankruptcy.

Thus, business security must be a compromise between ultimate security and ultimate business requirements. Such being the case, you can't possibly consider implementing any security policies without first examining how they'll impact your overall business operations, meaning you may as well just make your business policies and security policies all one set of policies.

The following list highlights some examples of how the common security compliance issues mentioned in the previous section might be reworded into more generic business policies:

- Permissions—Rather than creating security-specific policies for technology-based permissions, create a generic, business-level policy: *Only authorized individuals may make changes to business systems, resources, and processes, and each system, resource, or process must have a corresponding list of authorized individuals.* This policy makes sense not only at the network infrastructure level but also for electronic and paper documents, business practices, and so forth. In fact, this statement is a good summary of what most legislation—such as HIPAA and the Gramm-Leach-Bliley Act—are targeting.
- Reliability—A business-level policy about reliability might state that *all business processes must be documented and implemented in such a way that they cannot deviate from the documented standard.* Although such a policy seems like common sense, consider how this high-level policy might apply to network infrastructure devices. This policy doesn't allow room for misconfiguration, so the question of how to restore a device after a misconfiguration occurs is moot. Instead, this policy requires a proactive effort to *prevent* misconfiguration by only allowing the device to run approved configurations.

- Auditing—Auditing is simple to restate in business terms (and it is what most compliance legislation focuses on): *The company must retain records of all authorized and unauthorized access to corporate resources, systems, and processes.* It's simple, and it takes this important security concept right to the top, where it will affect *every* business process and system, not just IT.
- Standards—Restating this requirement in business terms plays well with the reliability concern: *All corporate processes and systems must be documented. Changes to documented standards will be made only by authorized groups or committees.* In fact, this type of policy really just takes the "standard configuration" and applies permissions to it.

All of this policy-making might seem pointless, but the real-world effect is significant. Look at these four common compliance concerns from a strict network infrastructure view and you get a complex set of rules stating who can modify devices, what configuration standards are preferred, and how devices can be reactively managed in the event of a problem. This state is, in fact, where most businesses are today with their network infrastructure security.

But if you restate these security issues as business policies and roll them into a common, overall set of corporate policies and standards, you get something much better. Reread the previous four bullet points as illustration of this point: *The company will develop and document standards that govern its operations. Only authorized parties can change those standards. All processes and systems will run according to those standards.* From a network infrastructure point of view, the practical implementation looks like this:

- Your organization will develop standards for network device configurations.
- The standard configurations will be enforced on all devices.
- Changes to the standard can be made only by authorized parties.

You might notice a lack of mention of authorized changes to devices. The reason is that there *aren't any such changes.* You stop managing devices. You've moved beyond low-level device management and into higher-level business management. Think about it: If your standard configurations are always being enforced, all you do is manage your *standard.* Change the standard and all devices are now out of compliance with it; your enforcement mechanism kicks in and reconfigures the devices to meet the *new* standard. You stop worrying about auditing individual administrators' actions on devices (although you still might want to do so) because those individuals' actions *don't matter.* Any changes will be undone by the enforcement process, which is managing the devices to the approved standard. Of course, finding the technology to actually implement this infrastructure can be complex—and is a subject of future chapters.

Planning for Compliance

So how do you begin planning for compliance at the network infrastructure level? The previous section provided clues, but in the next few sections, we'll walk through the process step-by-step. Keep in mind, however, that when I'm talking about "planning for compliance" I'm talking about *compliance with corporate policies.* It doesn't matter whether those policies relate to everyday operations or to security, and it doesn't matter if those policies were created internally or by a congressional act. Policies are policies, and compliance is simply the act of implementing those policies.

Creating a Top-Down Compliance Plan

Your first step will be to create a top-down compliance plan. By "top-down," I mean a business-level plan that focuses on business-level goals. Don't focus simply on technology. In this regard, HIPAA is a great example of what you should do: Although HIPAA recognizes that most health care records these days are kept electronically, HIPAA doesn't place an undue emphasis on the medium in which patient information is stored. Instead, HIPAA defines standards and controls for patient information *regardless* of its medium, meaning HIPAA applies equally to both physical and electronic documents.

Another way to look at it: Many companies create corporate security plans that go into great detail about how file servers must be configured to prevent unauthorized access. These same companies then allow employees to create hardcopies of those protected documents, and leave the hardcopies lying around on their desks, in trashcans, in unlocked filing cabinets, and so forth. Other companies write policies that require high-level encryption for any transmitted customer data but will fax that same data without any concern. The problem with these situations is that the companies are focusing on policies specific to a technology rather than focusing on the top-level, business perspective. Had they written policies such as *customer information will never be transmitted outside the building in any clear, easily-readable format,* faxing would suddenly be counter-policy and another solution would be found.

Thus, start planning by creating your policies at a high business level. From that point, you can begin creating more specific plans to implement those policies in a variety of ways. For example, you might implement encrypted email capabilities for customer information that is sent via email, while implementing some kind of encrypted fax line for customer information that has to be faxed; both are specific implementations of the higher-level business policy.

☞ Always write policies that describe the desired state of how things "shall" or "must" operate: *Customer information will be encrypted when stored or transmitted*, or *Business systems will operate only according to approved, documented standards*. This wording doesn't leave room for error and doesn't allow for a lag time between discovering a problem and fixing it; this wording will therefore drive a more aggressive focus on continuous compliance.

This top-down planning point is also where legislative requirements need to become involved. *Do not* open up the Gramm-Leach-Bliley A documents and start thinking about how to configure your network to comply with them; incorporate the requirements into your *own* comprehensive company policies, then you can start managing to that one, single set of policies. Once you've created (or updated) your company's own policies, there should never be a question of *are we HIPAA compliant*; the question should be *are we meeting company policies?* Because you know that your company *policies* are HIPAA compliant.

Planning for Auditing and Enforcement

Once you have your policies nailed down, you need to start thinking about how they will be enforced or, failing that, audited. At this point, you begin creating specific mechanisms to enforce your policies across the organization, such as adopting solutions that can provide automated enforcement of network device configurations or purchasing tools that can create centralized reports of file server permissions settings.

Your task at this point is to examine every policy and how it will affect every possible aspect of your business. This process is the one that most folks begin when they start reading HIPAA, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, or any other legislation; this is the actual *compliance* part of the process. It is important, however, that you should at this point be creating standards that will result in compliance, and thinking about ways to enforce (or at the very least audit) those standards; you should *not* have people running around reconfiguring things on the fly to come into compliance with your new policies.

Continuous Auditing vs. Point-in-Time Auditing

Point-in-time auditing is functionally useless as a compliance tool—it simply doesn't ensure compliance outside of that single point in time. Point-in-time auditing can tell you that you are, or are not, compliant *right now*. It says nothing about your state of compliance even 10 minutes ago, nor does it tell you anything about your compliance 10 minutes from now—let alone in a couple of days, weeks, or months.

People argue that point-in-time audits are useful as a form of checkup, but we're not talking about dentistry here. Twice a year is sufficient for your teeth because not many changes take place on a weekly basis. IT, and in fact businesses in general, change *every minute*. One administrator making one change to one network device's configuration can damage your compliance with every policy you've ever written, and a yearly, semiannual, or even weekly audit might not catch it.

The phrase *catch it* brings up another fault with auditing in general: It's too reactive. Auditing by its very nature implies that you will *find* a problem (potentially) and then *fix* the problem. It does nothing to *prevent* the problem, and in the interval between *find* and *fix*, there's plenty of opportunity for loss and damage to occur. The only type of auditing that is useful is *continuous,* automated auditing, conducted by some tool or technology. This type of auditing is still reactive, but because the automated the lag time between *find* and *fix* can be so small that it seems real-time, and because the auditing is automated and continuous, it's catching problems as they occur, rather than days, weeks, or months later.

Thus, you should rely on auditing *only* if you can implement automated, continuous auditing. Frequently, automated auditing is a component in automated enforcement, as well, and automated auditing and automated enforcement often come together in most tools and solutions.

Defining Rules

At this point, you've written your top-level policies, you've figured out how those policies apply to your network infrastructure and every other aspect of the company, and you've worked out some ideas about how to handle auditing and enforcement. Next, you can get serious about each system or process within your business by creating *rules.* For example, if you've got a business policy that, when implemented at the network infrastructure level, allows only HTTP and HTTPS traffic to leave the network, you can create a *rule* that specifies that firewall configurations must contain a port exception for HTTP and HTTPS traffic, and may contain no other port exceptions. You may also have a policy that requires a rule that disallows the use of the phrase *public* as an SNMP community string. These "use of technology rules" are very specific to a particular technology or system, and they're meant to support specific, high-level business rules.

Creating Policies

Finally, you bring everything full-circle by creating groups of rules that, for lack of a better word, you can call *policies.* These groups-of-rules "policies" should, in the end, match your top-level business-style "policies" (in other words, *This group of rules implements business policy number 107* or something like that). This process creates a comprehensible relationship between your business-level policies and the specific technological implementations that make those policies a reality.

Typically, you'll enforce and audit at the policy level. In other words, someone will pick up a big, thick company operations manual and read policy number 107, then want to know how that policy is being implemented on, say, your routers. Having defined the necessary rules and grouped them into "router policy 107," you can easily point out how the policy is being implemented. Should business policy 107 change, you'll know right where to go to update your routers to comply with the new policy.

Summary

We’ve covered a lot of philosophical ground in this chapter, but this foundation of knowledge is important for setting the stage for the future chapters. *Compliance* has been turned into a major issue, wrapped up with security and legislative controls, and has become unwieldy. By recognizing that compliance has always been around and that business policies are business policies no matter what they address, you can start to get a better handle on what companies and organizations are facing, and on how to deal with those challenges.

Consider compliance to be simply a matter of meeting your company policies and that your company policies incorporate *everything* you need to worry about: Internal rules, legislative controls, security requirements, and so on. In addition, make compliance a top-down effort, where you create standards that comply with your policies, then simply enforce those standards on various business systems and processes. To address the weaknesses in traditional auditing as a means of ensuring compliance, consider both automated auditing and automated enforcement as more robust solutions.

This information is a perfect lead-in to the next chapter, in which we’ll explore some of the traditional means of auditing and enforcement—means which may already be in use within your organization. The chapter will discuss some of their weaknesses, both from a business and compliance perspective, and set things up for the next chapters, which will show you how compliance *can* be accomplished in the 21st century.