



realtimepublishers.com<sup>tm</sup>

# *The Shortcut Guide<sup>tm</sup> 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](http://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](mailto:feedback@realtimepublishers.com), leaving feedback on our Web site at <http://www.realtimepublishers.com>, or calling us at 800-509-0532.

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.

Introduction to Realtimerepublishers..... i

Foreword..... ii

Chapter 1: Understanding IT Compliance ..... 1

What is Compliance? ..... 1

    Defining Rules ..... 1

    Meeting Rules ..... 2

    Enforcing Rules ..... 3

Verifiable Compliance ..... 6

    Doing vs. Being ..... 6

    Auditing vs. Enforcement ..... 8

Compliance and the Law ..... 9

    HIPAA ..... 9

    The Sarbanes-Oxley Act ..... 9

    21 CFR ..... 10

    Other Laws ..... 10

Compliance and Security ..... 11

    Common Security Compliance ..... 12

    Rolling Security into Overall Compliance..... 13

Planning for Compliance ..... 15

    Creating a Top-Down Compliance Plan ..... 15

    Planning for Auditing and Enforcement ..... 16

    Continuous Auditing vs. Point-in-Time Auditing ..... 16

    Defining Rules ..... 17

    Creating Policies ..... 17

Summary ..... 18

Chapter 2: Traditional Compliance Techniques ..... 19

Compliance and IT..... 19

Foundation Technologies..... 20

    Simple Network Management Protocol..... 20

    TACACS and RADIUS ..... 21

    Syslog..... 23

    Device Configurations ..... 24

    TFTP ..... 26

---

Foundation Methodologies .....	27
ITIL Overview .....	27
Traditional Compliance Management.....	30
Monitoring Only .....	30
Point-in-Time Audits .....	30
Manual Configuration Review.....	31
Template-Based Provisioning.....	31
The Shortcomings of Traditional Compliance Management.....	34
Vendor-Specific .....	34
Lack of Reporting .....	34
Alerting, Not Enforcement.....	34
Lack of Logging and Auditing.....	34
Entirely Manual .....	35
Not Real-Time .....	35
Lack of Accountability .....	35
Not Continuous .....	36
Summary .....	36
Chapter 3: IT Compliance for Today.....	37
Matching Business and IT Compliance .....	37
Defining Rules .....	37
Defining Policies.....	38
A Model Compliance Methodology .....	41
Defining the Business Process .....	41
Understanding the Supporting Technologies.....	44
Letting the Business Drive the Technologies .....	44
A Shopping List for Compliance Management .....	45
Vendor-Agnostic and Configuration Abstraction Tools.....	45
Reporting Capabilities .....	46
Logging and Auditing .....	46
Change Notification .....	47
Automatic Discovery .....	49
Dynamic Grouping.....	49
Real-Time Monitoring .....	50

---

Accountability.....	52
Enforcement.....	52
Rule and Policy Definitions.....	54
Update Capabilities.....	55
Solution Security.....	55
Summary.....	56
Chapter 4: Network Compliance Best Practices and Methodologies.....	57
The ITIL Framework.....	57
Network Compliance Management.....	61
Assemble Your Business Policies.....	61
Integrate Legal Requirements.....	63
Layer in Security.....	65
Create Your Final Business Policies.....	67
Applying Management Policies.....	67
Inventorying Your Network.....	67
Inventorying Your Needs.....	68
The Right Tool for the Right Job.....	68
Evaluating Management Tools.....	68
Matching Your Tools to Your Processes.....	69
“Do’s and Don’ts” for Network Compliance.....	71
“Do’s and Don’ts” for Network Security.....	72
Summary.....	72

## Copyright Statement

© 2005 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

---

## 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 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.

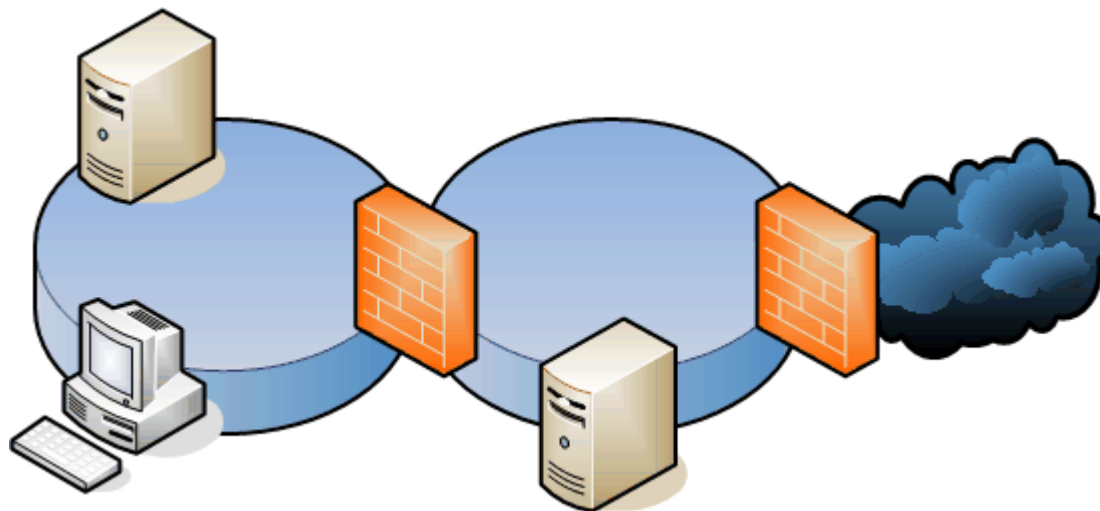


Figure 1.1: Sample network diagram.

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.

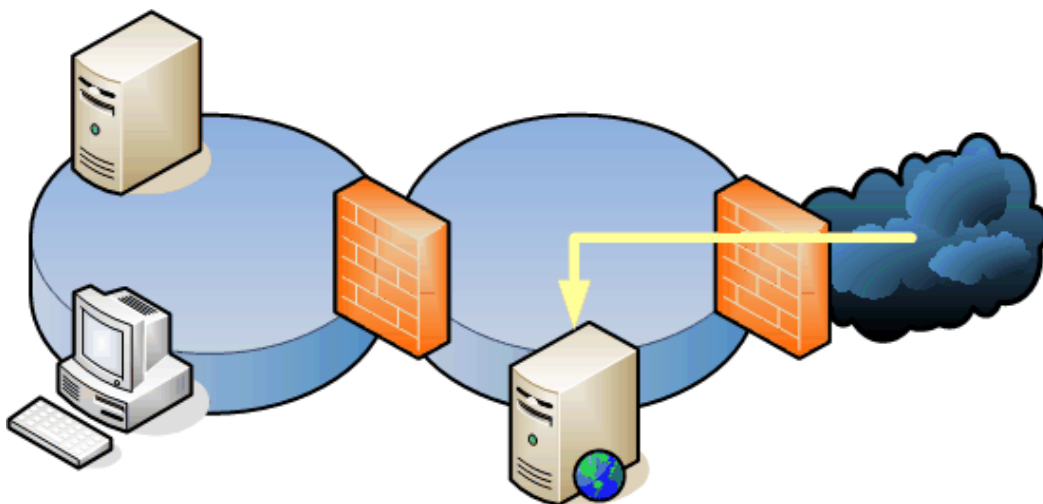
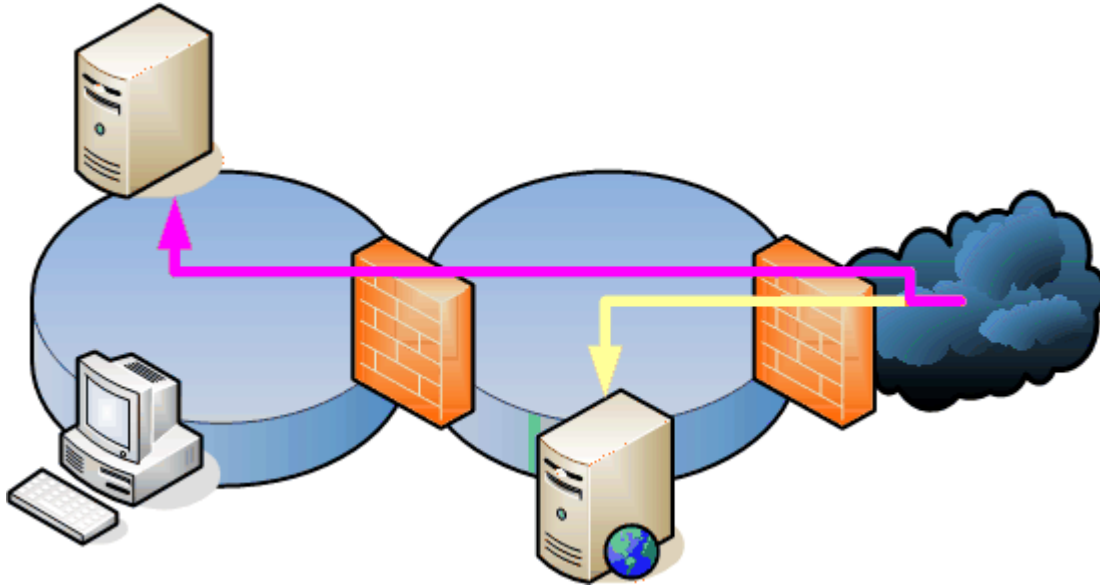


Figure 1.2: HTTP traffic is allowed to reach a Web server.

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

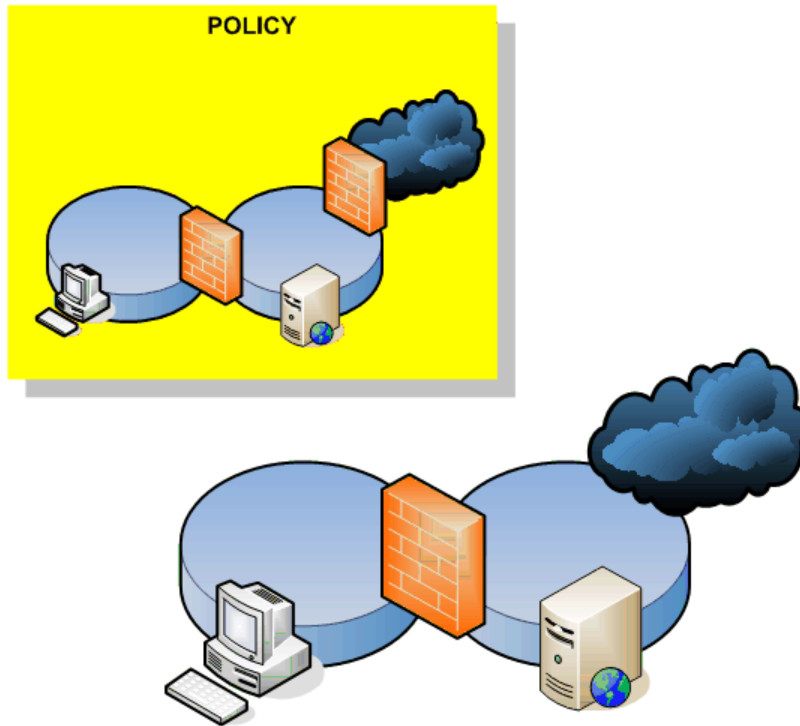
I've worked with a few clients who have developed comprehensive policies for how their network infrastructure should work, and spent tens of thousands of dollars configuring the network to meet those policies. But simply *doing* so doesn't tell you that you're compliant. And, while they had some great 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 device 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 21<sup>st</sup> century.

## Chapter 2: Traditional Compliance Techniques

*How do we make sure we're compliant?* It's an age-old question in the IT industry. As I mentioned in the previous chapter, *compliance* simply means obeying a set of rules; IT folks have been trying to obey rules long before legislative bodies such as the United States Congress and the European Union got into the act. Whether you're trying to comply with rules that relate to security, privacy, operational stability, or governance, knowing how to make your network compliant—and keep it that way—can be a complex task. In this chapter, we'll explore the traditional ways in which network administrators and engineers have dealt with compliance, and discuss how those ways help—and sometimes hinder—the overall compliance effort.

### Compliance and IT

One of the key issues in compliance management is how you verify compliance. As I described in the previous chapter, testing the *end state* is usually the preferred method. For example, if you have a rule which states that only certain individuals should have access to a specific piece of information, you conduct a test to confirm that no other individuals are able to gain access. This idea is simple enough in theory, but even in non-IT areas, it can be difficult to actually implement. For example, suppose you have a room in your office to which only certain individuals should have access for security reasons. How do you *prove* that nobody else in the world has a key? Dealing with IT-related compliance can be even more complex because it's often extremely difficult, time-consuming, or even destructive to test the end state. For example, testing certain security technologies would require an attempt to *break* those technologies; if you're successful at doing so, you have not only proven that the technologies didn't work but also damaged your environment.

Thus, instead of testing the end state, companies often rely on policy-based compliance. They create policies and procedures that will, if followed, guarantee a compliant end state. Then they simply audit and test to make sure that the policies and procedures are being followed. For example, if you have a policy which states that only certain individuals have access to a given locked room, you can audit the number of keys that were made for the room's lock and inventory the keys that have and have not been issued. This method audits the policy of issuing keys only to authorized individuals; in theory, provided all keys are accounted for, the end state of a secure room will be guaranteed.

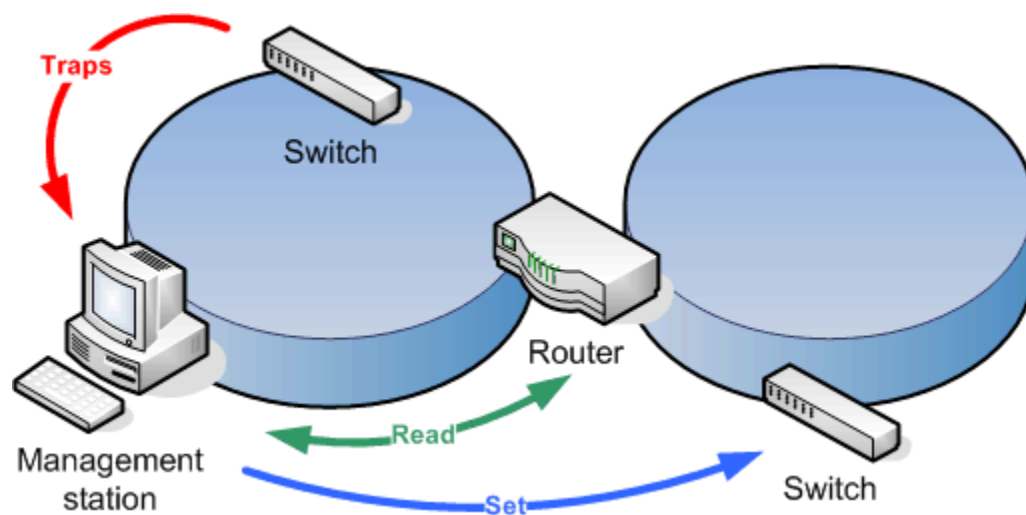
Most IT-based compliance, therefore, is based on compliant policies and procedures rather than on testing of end states. With network configuration management, this method of remaining in compliance is especially true, and several technologies exist to make policy auditing easier and more effective.

## Foundation Technologies

Over the years, several technologies have been created to help make network device management easier. Many of these technologies also lend themselves in one way or another to compliance management, although their relationship to compliance can be less than obvious. Still, understanding how these core technologies work, and what they offer both to compliance and general management, is important to understanding how compliance management can be made more effective.

### ***Simple Network Management Protocol***

The Simple Network Management Protocol (SNMP) was designed to make centralized management of network devices easier. Generally, an SNMP-enabled network consists of one or more SNMP *management stations* and one or more SNMP-enabled devices, such as routers, switches, and so forth. Figure 2.1 illustrates a typical network.



**Figure 2.1: SNMP in a typical network.**

As Figure 2.1 shows, the management station receives *traps*, or notifications, from managed devices. These traps often contain information about something that has just occurred, such as a configuration change, an error, and so forth. Management stations can process these traps and generate alerts for administrators or simply log the traps for future use. Management stations can also issue *reads* to devices, allowing the station to read certain configuration details from the device, or issue *sets*, which allow the station to change a device's configuration.

SNMP uses extremely simplistic security, primarily set through a *community string*. The community string is essentially a password; any management station possessing the correct community string can issue reads and sets to any managed device having the same community string. Newer versions of SNMP allow you to specify different community strings for read and set (or *write*) operations; this functionality provides for slightly more granular security control. For example, in a Cisco device's configuration you might see something similar to the following example:

```
Router#show running-config
....
....
snmp-server community public RO
snmp-server community private RW
....
....
```

This text specifies a community string of “public” for read operations, and a string of “private” for read-write operations. A drawback of these particular strings is that they're the defaults on almost every device in the world; thus, using “public” and “private” virtually guarantees that your devices' configurations will be available to anyone with SNMP software, regardless of whether a user is authorized.

From a compliance point of view, SNMP provides one important function—its traps allow devices to notify a central station when the devices' configuration might have changed. Any auditing activity can examine SNMP logs and, if traps are found, use those as a cue to perform a more detailed analysis on the devices involved.

### **TACACS and RADIUS**

Terminal Access Controller Access Control System (TACACS) and Remote Access Dial-In User Service (RADIUS) were originally conceived as a means of centralizing remote user access to networks. In the world of network management, however, they've become an important way to control administrative access to devices and to log access to devices. A typical network containing TACACS or RADIUS (although TACACS and RADIUS are different, the two serve the same function and work similarly enough that they can be discussed as a single technology) might look something like the network that Figure 2.2 illustrates.

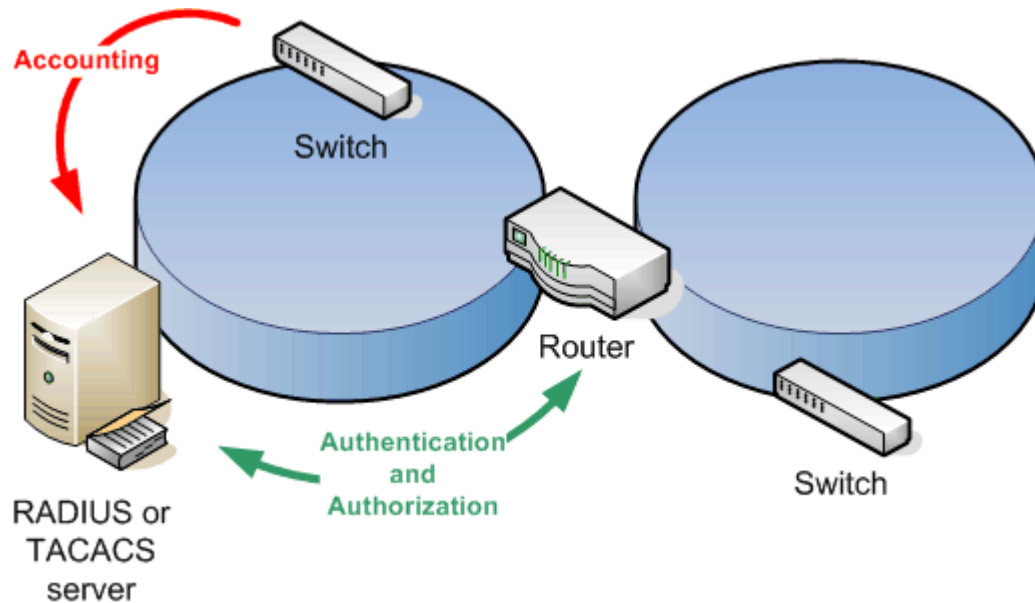



Figure 2.2: TACACS or RADIUS on a typical network.

When anyone attempts to gain access to a network device's configuration, the network device (if configured properly) passes the user's credentials to the RADIUS/TACACS server; the server responds with an *authentication* message indicating whether the user is who they claim to be (that is, the password is correct) and might also provide *authorization* information indicating which permissions the user has on the device. The goal of this process is centralization—rather than configuring each device with its own list of usernames and permissions, that information can be consolidated onto a single server and each device can simply look to that server for the information.

RADIUS/TACACS also provide valuable *accounting* features, allowing devices to send status information, security messages, and so forth to the RADIUS/TACACS server for long-term logging. This functionality is similar to that provided by SNMP traps, although most devices can generate more detailed RADIUS/TACACS messages than those provided by SNMP traps.

Devices must of course be configured to use TACACS or RADIUS. The following text shows an example of a script that configures a Cisco device to use a TACACS server.

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
ppp authentication default
```


 TACACS is popular in Cisco environments, as Cisco more or less owns the TACACS standard (which is currently referred to as TACACS+). RADIUS is a more vendor-neutral option.

TACACS/RADIUS plays an important role in compliance management. First, it is easier to maintain a compliant set of business policies (for example, user access permissions) when those policies are configured in one place—the TACACS/RADIUS server—than if they were configured in multiple places—on each individual device. Further, TACACS/RADIUS accounting logs can provide valuable auditing information, informing an auditor that a particular device might have been modified and leading them to review that device’s configuration in more detail.

### Syslog


Syslog is a mature logging technology supported by almost all network devices. Because network devices rarely have their own hard drives or other mass-storage devices, they are unable to generate and maintain local log files. The Syslog protocol was developed so that devices could transmit log entries to a remote server, which stores them for long-term use. Syslog files generally contain more detailed information than TACACAS/RADIUS or SNMP logs; logging detail can often be configured within a device to log packet-level information for debugging purposes, if desired.

As with SNMP and TACACS/RADIUS, devices must be configured to utilize a Syslog server. The following examples shows a Cisco switch configuration, illustrating that logging is enabled and directed to a server at IP address 192.168.1.100.

 The logging level and severity are configurable, controlling the number of log messages that will be generated.

```
set logging server enable
set logging server 192.168.1.100
set logging level all 5
set logging server severity 6
```

Like TACACS/RADIUS and SNMP, Syslog provides valuable logging and auditing information for compliance management efforts.

 It might seem like overkill for a single device to generate SNMP traps, TACACS/RADIUS accounting logs, *and* Syslog logs, but many organizations configure their devices to do just that. Syslog provides a continuous, low-level logging effort; TACACS/RADIUS accounting logs tend to focus on access control and administrative functions; and SNMP traps are often reserved for severe circumstances such as an error or possible device configuration change. There is a degree of overlap between the data captured in these technologies’ logs, but not enough to devalue each of their output.

## Device Configurations

Most network devices maintain their configurations in flash memory, meaning the configuration persists even if the device is powered off. The configuration itself is simply a text file, full of keywords that make sense to the device's internal firmware. Listing 2.1 provides a sample configuration file.

```

service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router1
!
enable secret 0 IMPORTANT!InsertYourPasswordHere!
!
clock timezone est 10
clock summer-time est recurring
!
dial-peer voice 1 pots
  caller-id
  no forward-to-unused-port
  no call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 1
  volume 3
  destination-pattern 0212345678
!
dial-peer voice 2 pots
  caller-id
  no forward-to-unused-port
  call-waiting
  ring 0
  no silent-fax
  registered-caller ring 1
  port 2
  volume 3
  destination-pattern 0287654321
!
pots country AU
!
ip subnet-zero
no ip source-route
!
ip domain-name insertyourdomainhere
ip name-server 139.134.5.51
ip name-server 139.134.2.190
isdn switch-type basic-net3
!
!
!
interface Ethernet0
  description connected to EthernetLAN
  ip address 192.168.1.1 255.255.255.0
  ip access-group 100 in
  no ip proxy-arp

```

```
ip nat inside
no ip route-cache
no ip mroute-cache
!
interface BRI0
description connected to Internet
bandwidth 128
no ip address
encapsulation ppp
no ip mroute-cache
dialer pool-member 1
isdn switch-type basic-net3
isdn voice-priority 0287654321 out off
isdn voice-priority 0287654321 in off
isdn voice-priority 0212345678 out always
isdn voice-priority 0212345678 in always
isdn incoming-voice modem
compress mppc
no cdp enable
!
interface Dialer1
description connected to Internet
ip address negotiated
ip access-group 100 in
ip nat outside
encapsulation ppp
no ip split-horizon
no ip mroute-cache
load-interval 30
dialer pool 1
dialer idle-timeout 3600
dialer string 0198308888
dialer hold-queue 10
dialer load-threshold 1 outbound
dialer-group 1
compress mppc
no cdp enable
ppp authentication pap callin
ppp chap hostname mybigpondaccount
ppp chap password 0 mybigpondpassword
ppp pap sent-username mybigpondaccount password 0 mybigpondpassword
ppp multilink
!
ip nat inside source list 1 interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
no ip http server
ip pim bidir-enable
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 100 permit ip any any
access-list 100 deny    udp any eq netbios-dgm any
access-list 100 deny    udp any eq netbios-ns any
access-list 100 deny    udp any eq netbios-ss any
access-list 100 deny    tcp any eq 137 any
access-list 100 deny    tcp any eq 138 any
```

```

access-list 100 deny tcp any eq 139 any
dialer-list 1 protocol ip permit
!
banner motd ^CUnauthorized users prohibited^C
!
line con 0
  exec-timeout 0 0
  password 0 password
  login
  stopbits 1
line vty 0 4
  access-class 1 in
  password 0 password
  login
!
ntp server 207.46.130.100
no rcapi server
!
!
End

```

**Listing 2.1: A sample device configuration file.**

As you can see, the file that Listing 2.1 shows is long and complex, which highlights one of the difficulties of compliance management—auditing these configuration files for the proper configuration values is a time-consuming, detail-oriented task that is frankly boring. Even dedicated auditors are likely to miss something. In an environment in which your organization is relying on proper configurations to maintain compliance, manually dealing with configuration files at this level is almost a guarantee that some compliance detail will be overlooked at some point.

For example, suppose you need to ensure that all routers are configured to traffic on TCP port 139. Can you determine whether the configuration that Listing 2.1 shows is compliant with this rule? To make this determination requires training, patience, and searching; imagine how boring it would be to verify this setting on a dozen—or a hundred—identical devices. Many organizations use more than one model or devices from different manufacturers—imagine that you must verify this rule in a dozen *different* configuration files.

### **TFTP**

Devices store their configuration files in an internal flash memory; working with this memory requires that you log on to the router through a Telnet or physical console session. This method is an inefficient way to work with device configurations, especially *en masse*. Fortunately, most devices also support the Trivial File Transfer Protocol (TFTP). By establishing a TFTP server on your network, you provide a place for devices to transmit—by using the TFTP protocol—their configuration files. The TFTP server can also act as a repository for new configuration files—devices can be commanded to load and use a configuration file that is located on the TFTP server.

Because TFTP represents one of the easiest and most common means of getting configuration files on and off of devices, it's a crucial technology in any network or compliance management effort. TFTP can be used to retrieve configurations for an audit, provide modified configurations to meet business rules, and back up and restore device configurations in the event of a disaster.

## Foundation Methodologies

Developing a methodology for compliance management can be difficult. Where do you begin? One approach is to use an existing foundation methodology that has been developed from industry best practices. The Information Technology Infrastructure Library (ITIL) is one common foundation methodology that is widely recognized in the IT industry for its adherence to and promotion of best practices.

### *ITIL Overview*

ITIL is a set of general IT best practices created by the United Kingdom Office of Government Commerce (OGC—<http://www.ogc.gov.uk/index.asp?id=2261>). ITIL addresses nearly every aspect of IT operations; of interest to compliance efforts is the ITIL sections on best practices for change and configuration management. The ITIL recommends a fairly comprehensive process of review, testing, deployment, and rollback, which are intended to prevent changes from having an adverse effect on the production environment. Figure 2.3 shows a sample business process developed from ITIL guidelines.

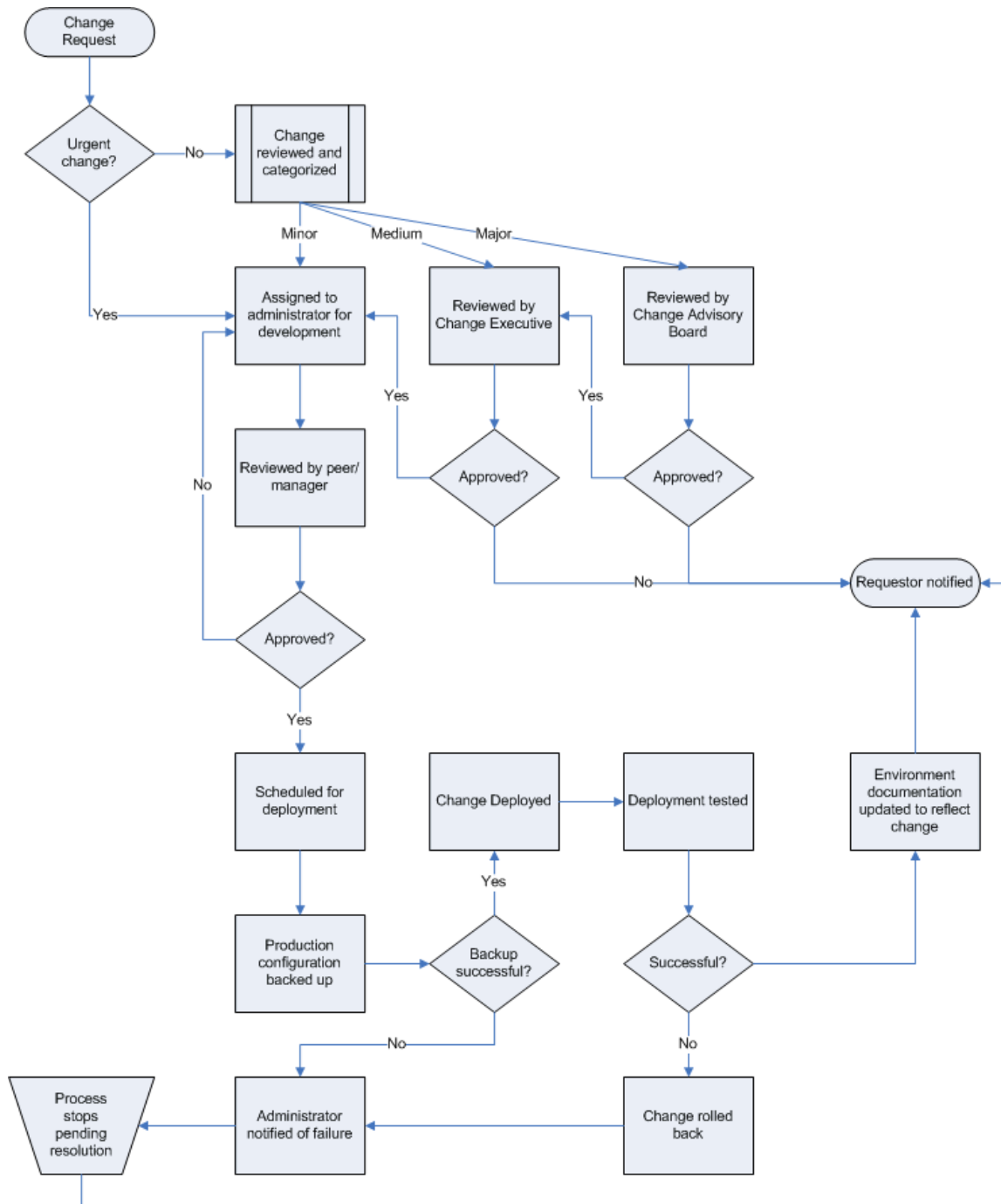


Figure 2.3: Sample change management process based on ITIL recommendations.

ITIL-based processes can form an excellent foundation for processes where compliance is a concern because the ITIL recognizes a few important facts about IT management in general (which happen to be especially true for network management):

- Changes to the production environment can often be easily made.
- Changes made to the production environment often take effect immediately.
- It is difficult to test an existing environment for compliance; it is easier to create configuration standards that are known to be compliant.
- By reviewing proposed configurations prior to their implementation, non-compliant configurations can be addressed prior to implementation, helping to maintain a compliant production environment.

ITIL also recognizes that IT management can become overburdened. ITIL therefore recommends a priority- and security-based categorization system that provides more thorough reviews for major changes as well as an expedited path for changes that are minor and less likely to have an adverse impact on either compliance or operations. In all cases, ITIL recommends peer or management review of changes to help ensure accuracy and mitigate simple human error.

Taking a moment to review the process in Figure 2.3, you can see that it offers several important aspects—both good and bad—to an organization concerned with compliance:

- The process focuses on catching non-compliant configurations *before* they are implemented.
- The process places an emphasis on post-deployment testing, including a rollback phase if the change's deployment doesn't go according to plan.
- The process does not focus on continual auditing of device configurations, a process which has already been identified as time-consuming and error-prone. Instead, devices are expected to be modified only through the process; of course, some means will need to be in place on devices to *enforce* the policy, ensuring that unauthorized (out-of-process) changes are detected and undone, or prevented entirely.


If ITIL has a weak point it's that it is a *process*, not a technology. In other words, the process must assume that you're using the process; no provisions are made for out-of-process events, which are the kind most likely to result in an out-of-compliance situation. Addressing out-of-process changes, however, isn't the job of a best practices system such as ITIL—it is your job to ensure that out-of-process changes simply cannot occur.

## Traditional Compliance Management

To ensure that out-of-process changes are eliminated, what are the traditional common practices used to manage today's networks for compliance? Keep in mind that *compliance* simply means “following business rules,” and that those rules will cover a spectrum of concerns—security, reliability, operational, and so forth—and may come from a variety of sources—internal rules, legislative rules, and so on. Let's explore traditional means of compliance management.

### Monitoring Only

Many organizations rely on monitoring to ensure that their network devices remain configured in a compliant condition. By *monitoring*, I don't mean periodic checks of the configuration—that would be *auditing*, which I'll discuss next. Monitoring is even more passive, simply waiting for red flags to be raised indicating that something is broken. Essentially, rather than checking the batteries on their smoke detectors, organizations are waiting for a fire to see whether the smoke detectors work. Of course, by then, you've got a *fire*. In other words, in order for monitoring to be effective, something has to be wrong, which means it's already too late.

 Monitoring is still, of course, an effective means of checking performance, activity levels, and other criteria; it's when monitoring is used as a compliance tool that it lacks value.

### Point-in-Time Audits

Another common compliance management practice is auditing—periodic spot-checks of device configurations to make sure that everything is set up according to plan. However, as Chapter 1 discussed, this method is ineffective. For example, how many people break traffic laws and never get caught compared with those who are issued a ticket? The discrepancy between these numbers illustrates the inefficacy of auditing: Officers can't be everywhere all the time, so they rely on spot-checks—*auditing*—to enforce the law. Do you want your organization's compliance to be as ineffective as traffic law enforcement?

Auditing tells you that everything is—or is not—compliant *right now*. It says nothing of 10 minutes ago, 2 days from now, or at any other point in time despite the fact that networks are dynamic, constantly changing entities. The network that is audited today *will* be different tomorrow, yet today's audit won't be at all concerned with the network's state of compliance tomorrow.

However, there are situations in which auditing could be useful: If an auditor could be called in each and every time a device's configuration was changed, the auditor would then have the opportunity to audit the environment each time it changes, ensuring that each new iteration of the environment is as compliant as the last one. Obviously, such is not the case, and auditing remains an ineffective way to manage compliance.

### **Manual Configuration Review**

Too often, auditing is based on manual reviews of network configuration files. As I've already described and illustrated, this time-consuming, error-prone process will rarely result in consistent audit results. Thus, in addition to the uselessness of auditing as a compliance tool, the audits aren't even accurate and consistent.

This is not to suggest that a review of configuration files isn't beneficial; it is the only practical way to create a compliant network because end-state testing is so impractical. What I am proposing is that the complexity of these files, and the room (and likelihood) for human error in a configuration file review makes a *manual* review less likely to ensure compliance.

### **Template-Based Provisioning**

Template-based provisioning is a fairly new technique in network management and promises better compliance results. The idea is simple: Create a template of a known-good configuration that is compliant with all of your business rules. All devices are then configured based upon that template. Auditing can begin with a simple automated comparison of a live configuration file with the template that the file is supposed to be based upon; anything in the configuration that matches the template is compliant and can therefore be ignored; auditors can then focus on only the differences. The differences represent a much smaller area on which to focus, lessening the tedium of a manual review and increasing the level of accuracy and consistency.



Manually performing this comparison is still a point-in-time audit; additional measures, including automated enforcement (which the next chapter will discuss), build on template-based provisioning to provide a more reliable compliance solution.

For example, suppose the text in Listing 2.2 is a part of an approved, known-to-be-compliant device configuration template.

```
ip classless
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
!
tftp-server flash:
snmp-server community corp_orate RO
snmp-server location HCC-Atlanta
snmp-server contact Joe,555-1212,joe@company.com

banner motd #Welcome#
!
line con 0
  exec-timeout 0 0
  password 7 094F471A1A0A
  login
  transport input none

line aux 0
  password 7 070C285F4D06
  login

line vty 0 4
  password 7 01100F175804
  login
!
```

**Listing 2.2:** A sample of an approved, known-to-be-compliant device configuration template.

Next, suppose that the text in Listing 2.3 is the same portion of an actual configuration file.

```

ip classless
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
!
tftp-server flash:
snmp-server community public RO
snmp-server location HCC-LasVegas
snmp-server contact Joe,555-1212,joe@company.com

banner motd #Welcome#
!
line con 0
  exec-timeout 0 0
  password 7 094F471A1A0A
  login
  transport input none

line aux 0
  password 7 070C285F4D06
  login

line vty 0 4
  password 7 01100F175804
  login
!

```

**Listing 2.3:** A sample portion of an actual configuration file that is supposed to be based on the template that Listing 2.2 shows.

A simple comparison utility would reveal the differences between the template and the live configuration:

Template:

```

snmp-server community corp_orate RO
snmp-server location HCC-Atlanta

```

Configuration:

```

snmp-server community public RO
snmp-server location HCC-LasVegas

```

One of these differences—the change of the location to LasVegas—might be documented as an acceptable deviation from the template. The other, however, is a security-sensitive setting that configures the SNMP community string. The ability to focus on only these two lines will enable an auditor to more easily catch a non-compliant configuration setting that might otherwise be lost in a file that contains hundreds of lines of configuration settings.

## The Shortcomings of Traditional Compliance Management

Simply by reading the previous few sections, you've likely spotted a few problems with these traditional compliance techniques. However, there's more wrong than meets the eye.

### **Vendor-Specific**

One major problem with many compliance efforts is that they're vendor-specific. Training auditors to look at configuration files, for example, is a vendor-specific task, meaning companies with more than one vendor's equipment will need to train auditors on each. Even management solutions provided by vendors are specific to that vendor's equipment.

To resolve this problem, companies need to employ a management solution that is vendor-neutral and supports a broad range of manufacturers' equipment. The ideal solution will create an abstract version of device configurations so that every configuration setting looks the same, regardless of which manufacturer's device it came from. This abstraction—or translation, if you will—helps to homogenize the configurations and make them more easily audited or modified.

### **Lack of Reporting**

Because traditional compliance management is largely manual, no automated reporting is available. However, even most automated configuration management tools lack reporting capabilities. For example, a solution that backs up device configurations should be able to produce reports that list devices whose configurations have changed since the last backup; such solutions rarely provide this level of reporting, however. Foundation technologies that support compliance effort often lack reporting, too. Having a RADIUS/TACACS solution produce a report that lists all administrator access to a device might be a useful tool for judging whether the device needs to be re-audited; too few of these solutions lack such reporting capabilities, making them less supportive of techniques that would result in better compliance.

### **Alerting, Not Enforcement**

Alerting is a common way for organizations to keep tabs on their environments, but alerting is too slow. By the time an alert has been produced, a problem already exists and must be corrected immediately. Enforcement combines alerting with an automated, immediate response—perhaps rolling back a device configuration to a known-compliant version—which *ensures* compliance rather than simply alerting to you to *lack* of compliance.

### **Lack of Logging and Auditing**

Centralized network configuration tools often lack sufficient logging and auditing capabilities. Although these tools provide centralized control over devices, which is a crucial component for easier compliance management, the tools are not often designed to keep track of what centralized changes are made and by whom. This shortcoming essentially removes the tool's usefulness as a compliance management tool (although not as a network device management tool, which is in fact what most such tools are built as).

### ***Entirely Manual***

Most compliance efforts, in the end, are entirely manual. Manual processes are all subject to human error and inconsistency and are therefore less preferable than automated processes. Ideally, every manual process in your current compliance management efforts is replaced, at some level, by an equivalent automated process:

- The process of comparing device configurations to known-compliant templates should be automated.
- The process of rolling back configurations to a known-compliant state should be automated.
- The process of auditing devices each and every time their configurations are changed should be automated.

With automated processes, manpower, time, and money become non-issues, and compliance can be more consistently ensured across the network.

### ***Not Real-Time***

Traditional compliance management—which relies heavily on auditing—isn't real-time in nature. Instead, it tends to focus on point-in-time audits, which don't reflect all the changes that can occur from moment-to-moment on a production network. Capturing changes in real-time is critical because being out of compliance for even a moment can result in enormous losses; realizing that you have changes occurring can even help you redesign your network and security to help prevent those changes from occurring.

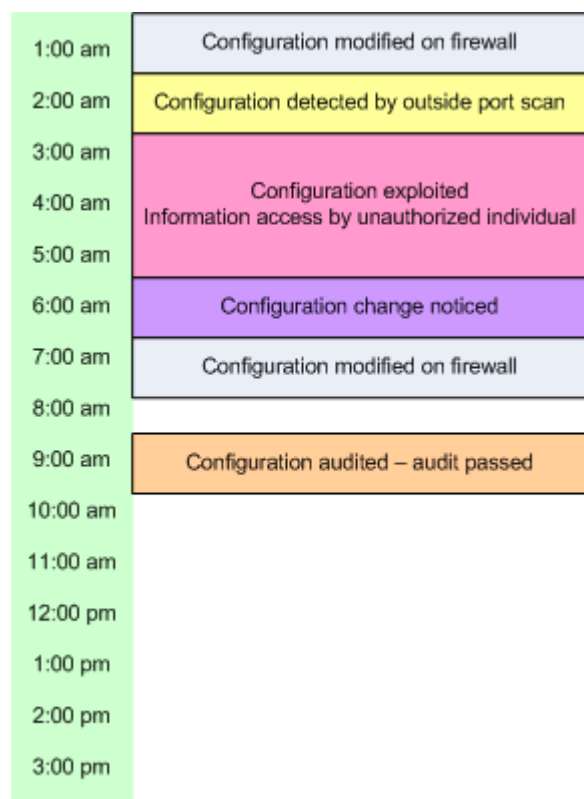
### ***Lack of Accountability***

Many traditional compliance management methods seek to establish accountability, in large part as a result of the many pieces of legislation that now mandate accountability (HIPAA, Sarbanes-Oxley, and so forth). Traditional compliance management, however, often fails to achieve this accountability at the network device level. Network devices are notoriously difficult when it comes to accountability because few of them lack any built-in means for tracking who makes what changes. Most devices support external technologies, such as TACACS or RADIUS, which can provide accountability, but these technologies often make it difficult to tie the *who* with the *what*: Although RADIUS can, for example, let you know that an administrator logged onto a router's console, RADIUS can't generally detail the exact changes that administrator made because RADIUS (and the network device) simply wasn't designed with that level of granularity. As a result, accountability for network management is often slipshod or inaccurate.

## Not Continuous

Traditional compliance management is manual, lacks supportive reporting capabilities, and tends to be vendor-specific, so it cannot be continuous. Any compliance effort that isn't continuous—which, in other words, relies on spot-checks—is next to useless because networks simply change and evolve too quickly for spot-checks to have a hope of catching non-compliant conditions.

Your network needs to be non-compliant for only a few minutes in order for security breaches, operational problems, reliability issues, stability concerns, and other problems to occur. Fixing the problem quickly doesn't negate the fact that a problem occurred and damage was done; only *continuous* compliance management can truly be effective. The timeline in Figure 2.4 shows how non-continuous compliance management leaves plenty of room for problems to occur.



**Figure 2.4:** Timeline showing how an audit can miss a non-compliant configuration as well as the resulting damage.

## Summary

Thus, if every traditional compliance management technique—monitoring, auditing, alerts, manual configuration reviews, and so forth—doesn't provide adequate compliance assurance, what does? Chapter 3 explores the answer to that question: Leading-edge techniques for providing real-time, information-rich, and highly automated compliance management. You'll rely on the same foundation technologies—SNMP, Syslog, TACACS/RADIUS, configuration files, and so forth—that this chapter has introduced, but you'll replace spot-checks, error-prone manual reviews, and other traditional techniques with new solutions that make compliance more automated and more consistent.

## Chapter 3: IT Compliance for Today

One of the reasons that compliance management has become such a boom business for consultants is that companies know their existing techniques often aren't sufficient to meet compliance requirements. Worse, companies often aren't even sure how regulations—such as HIPAA, the Sarbanes-Oxley Act, 21 CFR, and more—even apply to their technological assets. Too often, regulation requirements are dumped onto technical professionals for implementation, leaving those professionals confused and frustrated about what they are supposed to do. It doesn't have to be this way—with the help of a few useful tools, compliance can be easy and straightforward and enable your organization to focus on business instead of these mandatory rules.

### Matching Business and IT Compliance


One of the most irritating and frustrating situations for a technical professional is to have a manager dump some new, arbitrary set of rules on them without explaining what they mean or why they must be applied. Yet that is what many managers—themselves confused by how legislation applies to the business—wind up doing. The result is confusion, frustration, inefficiency, and often poorly implemented compliance. Technical professionals are accustomed to implementing business policies, working with a single set of rules, and translating those rules into technical requirements; you should approach compliance the same way.

#### Defining Rules


Think of a *rule* as a single business or technical requirement. For example, the requirement that *Network device configurations must not be modified or viewable by unauthorized personnel* is a business requirement that meets both typical business needs as well as many compliance needs. A technical rule that you might develop from this requirement is *SNMP community strings must not be “public” or “private” because those strings are too well known and would allow an unauthorized individual to view or modify device configurations*. These examples illustrate a well-stated business rule coupled with a well-stated technical implementation of that rule. A technical professional can easily understand and implement this technical rule.

It is at this level that management should communicate compliance requirements to technical professionals. Although managers might not be able to translate legal compliance requirements into technical requirements, they can at least take the middle step of translating compliance requirements into simpler, clearer business requirements. Network administrators can then create the corresponding technical rules.

For example, if the regulation you're working with has a somewhat vague (from a technical perspective) requirement such as *Patient data cannot be disclosed unless that disclosure is logged*, you might translate that requirement into a clear business requirement that states *Absolutely no access to patient data is permitted unless that access can be permanently logged. If logging capabilities are unavailable, then patient data cannot be accessed.* This clear business statement resolves a potential conflict between the regulation (logging required) and the typical business need for continuous data access. A technical professional might interpret the regulation by itself simply to mean that auditing of files is required; with the clearer business statement, the technical professional knows that steps must be taken to ensure that auditing is online and functioning whenever data access is permitted.

 Compliance requirements can sometimes seem to conflict with previously stated business requirements. Compliance often focuses on security and accountability, while the business has an obvious need to focus on efficiency, cost, and other concerns. The conflict between the two can create technical results that are often bad for both compliance and the business. The solution? At a management level, create a single, comprehensive set of policies that address both business and compliance requirements and resolve any conflicts between the two. Provide this single set of rules to your technical professionals for implementation. We'll explore this idea in more detail in Chapter 4.

Rules should be as granular as possible. Technical rules, in particular, should be extremely granular and should generally apply to a single configuration parameter or setting within one or more network devices. Granular rules are modular and are easy to build policies around.

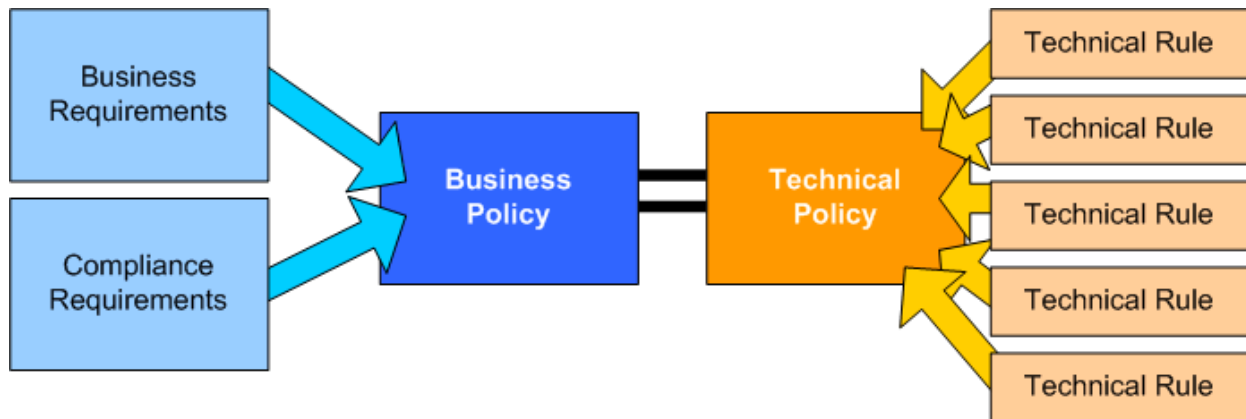
 Although this terminology is a little abstract, it serves to help define the basic compliance concepts. A *rule* is a single piece of configuration work; rules combine—as you'll see next—into *policies*, which govern the total configuration of one or more devices. These policies create mappings to business-level rules and regulations, which help ensure that devices are managed directly by business and regulatory requirements.

### Defining Policies

A *policy* is a collection of rules that you want to enforce. At a technical level, policies are enforced to particular network devices, such as routers or switches. Policies should map in a general way to your business and compliance requirements. For example, suppose your company policies state that all network device configurations must be viewable and changeable only by authorized personnel, and that authentication and authorization to those devices must be centralized and audited. This fairly common requirement meets several compliance and business needs. Several rules go into this policy—especially at the technical level:


- SNMP community strings must be non-default (for example, not “public” nor “private”)
- Access control lists (ACLs) must be applied to the network devices
- The devices must be configured to use TACACS or RADIUS for authentication, authorization, and accounting

These rules, then, form a technical policy that corresponds to and implements the business-level policy. This technique creates a one-to-one mapping between business-level policies (which include compliance requirements) and the technical rules and policies that implement and enforce those business-level policies. By having the technical policy consist of multiple granular rules, the technical policies can be implemented and enforced more easily. Figure 3.1 illustrates the relationships between these components.



**Figure 3.1: Mapping business policies to technical policies.**

Why bother with this sort of one-to-one mapping? The answer is easier management. Tools exist, for example, that can monitor and enforce groups of technical rules. By creating rule groups that correspond to business policies, you can more easily verify that your environment is meeting with your business policies. Your business policies incorporate compliance requirements, so meeting your business policies means that you are meeting your compliance obligations. In effect, the tools will ensure that you're meeting your compliance obligations.

 This sort of “top-down” management—managing via policies and having tools that enforce the policies—is becoming more popular in today’s enterprises. Hewlett-Packard Adaptive Enterprise, IBM OnDemand, Microsoft Dynamic Systems Initiative, and other major frameworks are built around the concept of policy definitions driving actual provisioning and configuration management. When the business needs change, you simply rewrite your policies and your enterprise reconfigures itself to match.

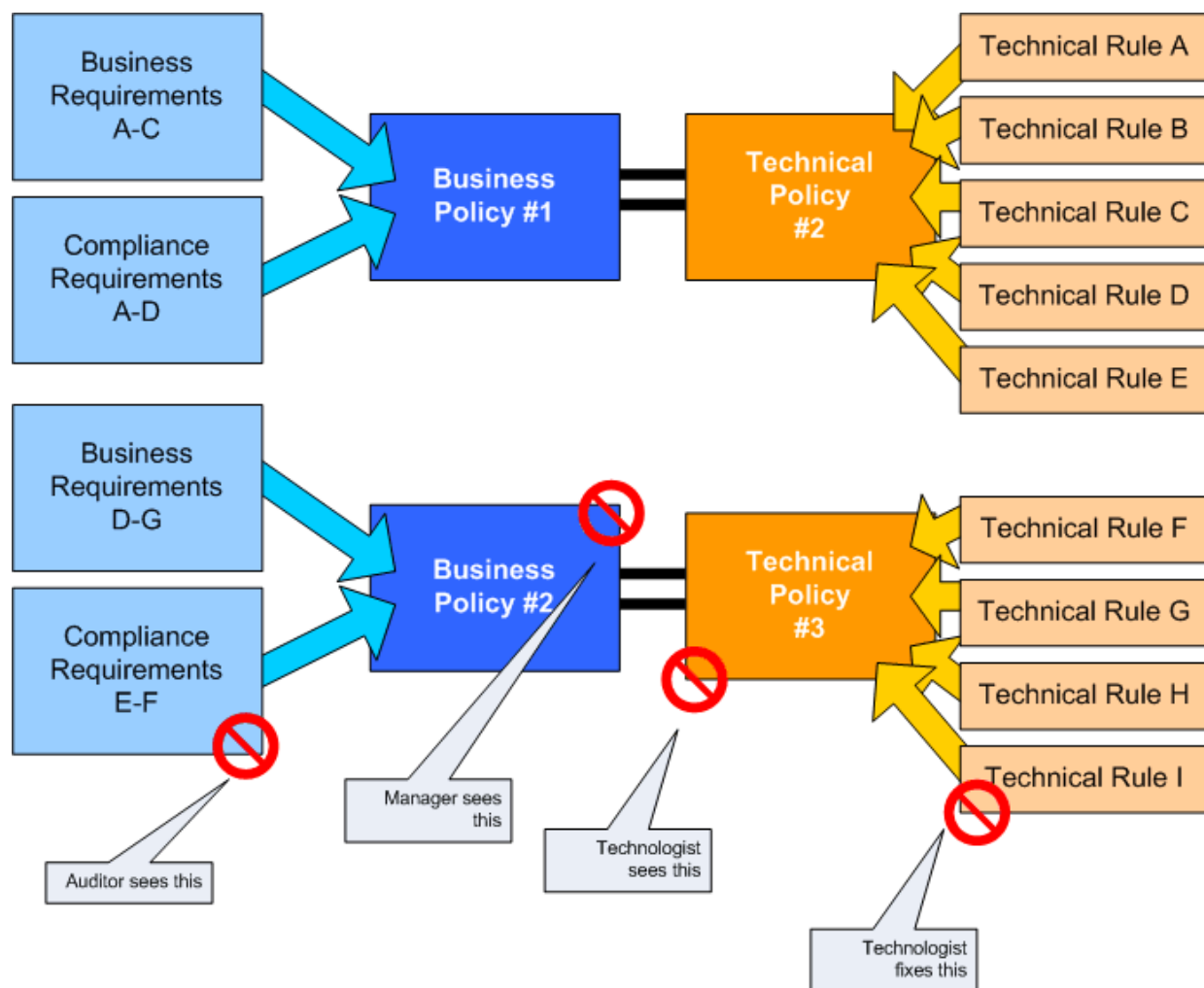
Without grouping these technical rules into units that correspond to business policies, however, you will constantly be in the state of having to match rules to compliance requirements. For example, staring at a report that says *No devices have an SNMP community string of “public”* might be interesting data, but it’s not valuable information. Having a report that says *Our device access requirements are all being met* is much more useful information because it corresponds directly to a business or compliance requirement.

### Data vs. Information: What Is the Difference?


The terms *data* and *information* are often used interchangeably, but they have distinctly different meanings. *Data* refers to raw facts without any context. For example, the statement *We added 1000 subscribers last year* is data. It is interesting but doesn't tell you anything useful about business performance. Placing data into context turns it into information: *Our subscriber base grew by one-half of one percent last year, which is seventeen percent less than the year before.* This statement is meaningful—information often comes from the distillation and combination of several pieces of data. From a compliance standpoint, your reports should help translate data—individual points of compliance—into meaningful information about your overall level of compliance.

The same holds true coming from the other direction. Looking at a report that says *Our devices do not meet our access requirements* is a red flag for a manager who must then assign technical professionals to address this problem. Those professionals can look at the rules comprising that technical policy and determine exactly which bit of the devices' configurations is wrong.

Troubleshooting is made more efficient because there is a direct correlation between business policies and technical configurations. Figure 3.2 illustrates how troubleshooting can be made easier through this organization of rules and policies.




**Figure 3.2: Creating mappings between business and technical policies creates more insight for each level of an organization.**

 The mapping between business and compliance requirements to technical rules and policies makes compliance management much easier. When something is out of compliance, it is easy to determine which technical rules are being violated and fix the problem because your organization will have defined each configuration setting that is responsible for a compliant environment. The mapping also makes it more feasible for auditors to test the end state—that is, the actual working conditions—of your compliance rather than focusing solely on technical configuration elements that result in compliance.

## A Model Compliance Methodology

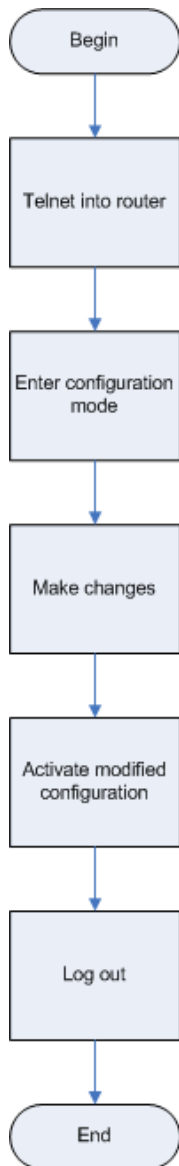
Determining how to methodically approach compliance can be complicated and intimidating. It is, however, the only way to ensure accurate compliance. Ad-hoc efforts will invariably leave holes in your compliance because ad-hoc efforts aren't comprehensive and methodical. The implementation process all starts with understanding how you do business and how your compliance requirements will affect the way you do business.

 I once worked for a company that was developing a new software application to support their network consulting business. The IT staff had created a pilot application and asked the various managers in the company to review it and offer feedback. In a meeting, one manager pointed out that the application should import drawings from the drawing software his engineers used. A second manager disagreed, saying they didn't really use that software even though they had bought it. A third said that they did use the software, but only for drafts.

The software developers were at a loss. With even the company's managers unable to agree on how they did business, how were the developers supposed to create something that would meet their needs? Fully understanding and defining how you do business is a critical part of any technological solution, and that includes bringing your technical resources into legislative compliance.

### *Defining the Business Process*

Start by clearly defining, in deep detail, how your various business processes work. If your company is International Standards Organization (ISO) 9001 certified (or certified in a similar process-management methodology), you have probably already defined the workings of your business processes by developing detailed process flowcharts. Those charts will be useful, but they need to be modified to reflect changes mandated by legislative compliance requirements. For example, Figure 3.3 shows a simplified flowchart of how a network administrator might have accessed a router's configuration prior to compliance requirements being an issue.



**Figure 3.3: Pre-compliance router configuration process.**

Figure 3.3 is a simplistic business process; one that many organizations use: create the change, then implement the change. This process is not a *manageable* process, nor is it typically a process that will meet regulatory requirements. Figure 3.4 shows the same process but with the additional compliance requirements of authorization and access added to illustrate how these become part of the process.




### **Understanding the Supporting Technologies**

Obviously, some feedback from technical professionals is necessary when developing policies because you need an understanding of what the technology can do and the restrictions it might place on your business flexibility. For example, creating a business requirement that all router access must be authenticated by two-factor authentication (such as a smart card or biometric system) is fine, but that requirement might restrict administrators' ability to log on from remote locations at which the two-factor technologies aren't available (for example, when they work from home). You can then make a business decision about whether such flexibility is desirable or necessary.

An effective practice is to start with the business requirements that you would prefer to have implemented regardless of the cost or practicability, then back off depending on the capabilities of the technology or based on the restrictions the technology might place on business requirements. Working out business requirements first ensures that the business is in control, not the technology.

### **Letting the Business Drive the Technologies**

Allowing technology to drive the business is not a good practice. For example, suppose network administrators are given a requirement that says *No users must be able to access a router's configuration without authenticating*. In response, the administrators simply pull the plug on the router because no one can access a router's configuration when the router is turned off. Although, technically, the requirement has been met, the means of doing so is not good for the business. Thus, you need to state *business* requirements, and let the *business* drive the technology; avoid creating policies that state *technical* requirements, because then you're letting the technology do the driving.

 One perceived problem with letting business drive technology is that some business requirements might call for tools that are expensive. If the technology needed to support your business is prohibitive (either in terms of cost or some other factor), you can review the business requirements and make changes. In that case, you're making a conscious decision to change the way you do business to make it more manageable or less expensive; this method is not letting the technology drive the business, it's making smart decisions about the way you do business.

If you discover that your current technologies can't precisely meet a business requirement, you can make a business decision to change your requirements or acquire technologies that can do what you want. In either case, it's the business, not the tools, making the decision.

Most organizations today lack the technologies and tools to adequately ensure compliance. As previous chapters have described, organizations are relying on point-in-time audits, homegrown tools, and tools intended for other purposes to maintain a legally compliant network infrastructure. In addition, they often allow the limitations of their technologies to limit what their business can do while remaining compliant. Instead, acquire tools that are designed to support compliance management, ensuring that your business can be effective and compliant.

## A Shopping List for Compliance Management

An interesting fact about the tools available to help manage compliance in your network infrastructure: The tools exist, but in many cases, their manufacturers are just starting to realize their products' value in an environment that requires compliance. In other words, everything you need has more or less already been made and released to market, although it might not say "compliance" right on it. Thus, it is important to understand what underlying capabilities a good network compliance management tool will have so that you can recognize these features even if they're not specifically billed as being useful in a compliance effort.

### *Vendor-Agnostic and Configuration Abstraction Tools*

Unless you work for a company that manufactures network devices and therefore quite reasonably only uses their own brand of device, the odds are that your network infrastructure consists of several vendors' products. Routers and switches are commonly from different vendor, as are firewalls, proxy servers, and so forth. Using vendor-specific tools—typically provided by the vendor, in many cases—means your staff will need to learn multiple tools, deal with tools that have varying capabilities, and, in general, work with a mishmash of products that create inconsistent results.

In contrast, using vendor-agnostic tools, your team can learn to use a single toolset to get the job done, and the tool will be able to perform consistently across every device. The result: less training, less administrative overhead, and more consistent results across the enterprise. You will also enjoy fewer configuration errors, fewer misinterpretations of requirements, and so forth.

Even better are vendor-agnostic solutions that abstract vendor-specific data into a more generic format. For example, a network configuration management tool can take one of two approaches when configuring devices: It can simply display the configuration as-is, in its vendor-specific format, or it can parse that configuration and present it in a more generic form. The benefit to the latter technique is that all devices, no matter what their purpose or manufacturer, wind up looking the same. Again, this means less training for your network administration team because they are looking at a single data representation and don't need to learn to read different vendors' native configuration formats. They also get more consistent configuration results and fewer configuration errors.

For example, many devices will set their SNMP community strings with a configuration line as follows:

```
snmp-server community public RO
snmp-server community private RW
```

Others, however, will use a slightly different syntax:

```
snmp-community public RO
snmp-community private RW
```

Rather than expecting your network administrators to remember these differences—and the differences become more significant with more complex settings—you can use tools that understand that differences and present the information in a uniform, generic format. The result is a more consistent configuration because all devices can be dealt with on an equal, uniform basis.

## **Reporting Capabilities**

Look for solutions with robust reporting capabilities. Although it is easy to focus on solutions that offer compliance-specific reports—such as reports that report whether your organization is compliant with the Sarbanes-Oxley Act, you should become accustomed to looking more closely at the reports a solution offers. Many solutions, for example, offer reports on recent configuration changes that make perfect Sarbanes-Oxley Act compliance reports, even though those reports aren't specifically labeled for Sarbanes-Oxley compliance. More astute manufacturers are catching on to compliance and providing labeled reports to assist with compliance efforts, but remember that by and large these tools have been around and evolving since before compliance was a big issue.

What specific type of reports should you look for? Ideally, a single-click report that details changes made to your network infrastructure. If the tool provides a workflow for change management (an excellent feature to look for), reports should highlight changes that were made through the workflow and changes that weren't; the latter category of changes is the one you'll need to pay special attention to because these changes represent exceptions to your change management process and might represent compliance concerns.

## **Logging and Auditing**

Logging and auditing is at the heart of compliance management, because most legislation focuses at least partly on accountability, which is provided through logging and auditing. Most solutions rely on their own internal databases for logging and auditing, which is a useful feature; more generic logging capabilities provided by technologies such as RADIUS aren't always suitable for capturing the level of detail you want in network configuration management.

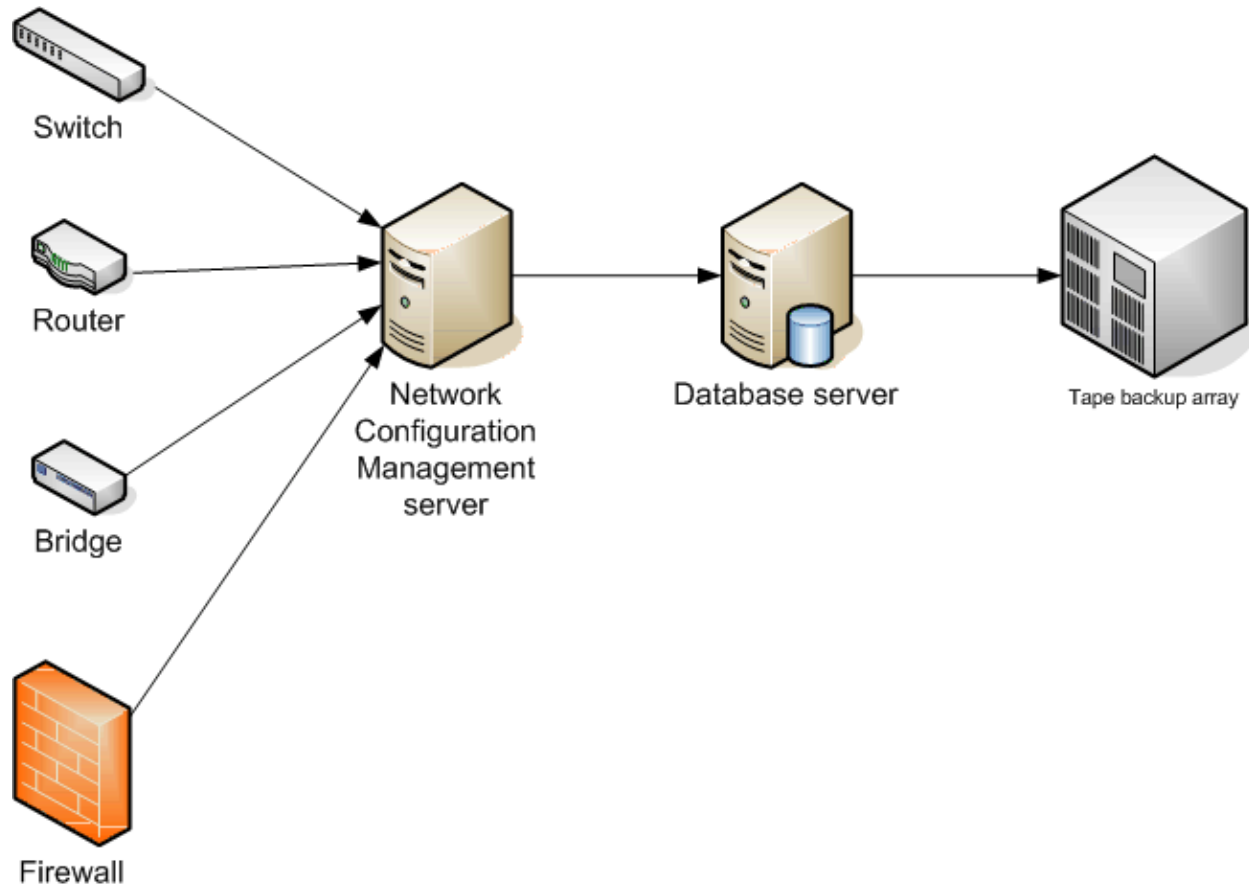
For example, when an administrator makes a change to a device, your network configuration management solution should capture the administrator's identity (such as his or her user name), the time and date of the change, and ideally both before and after snapshots of the device's configuration, or at least details about the exact portions of the configuration that were changed. This level of logging and auditing provides all the evidence you need for any compliance effort, and should provide sufficient data for almost any type of report the solution might need to provide.

Logging and reporting are closely tied: If a solution doesn't have a robust logging capability, then its reports—which simply pull from those logs—won't be robust either. Look for solutions that log to a database rather than a flat file. Databases might be proprietary or use industry-standard such as Oracle, MySQL, Microsoft SQL Server, and so forth. The latter are preferred as you will be able to use standardized means of securing, backing up, and maintaining your databases.

Figure 3.5 illustrates a solution that uses a back-end database server, which is maintained and backed up by an independent solution. Databases provide scalability and reporting capabilities and can generally be made part of an enterprise disaster-recovery scheme more readily than plain files can. Most important, however, is the reporting capabilities. With data stored in a flat file, it is more difficult to generate complex, robust reports; with data stored in a database, you will have a much wider range of options for generating the reports you need to manage your enterprise more effectively.

The ability to use an external database is essential. Although internal, proprietary databases are preferable to a flat file or other less-efficient means of data storage, an external database is typically more securable and more scalable, can fit more easily into an enterprise data maintenance plan, and can be made more fault- and disaster-tolerant.

👉 Look for solutions that support multiple database back ends so that you can use an existing database server or at least use a database product that your technical staff is comfortable supporting. If your staff, for example, knows MySQL, introducing a network configuration management solution that only supports Microsoft SQL Server will add a whole new layer of complexity to your environment.



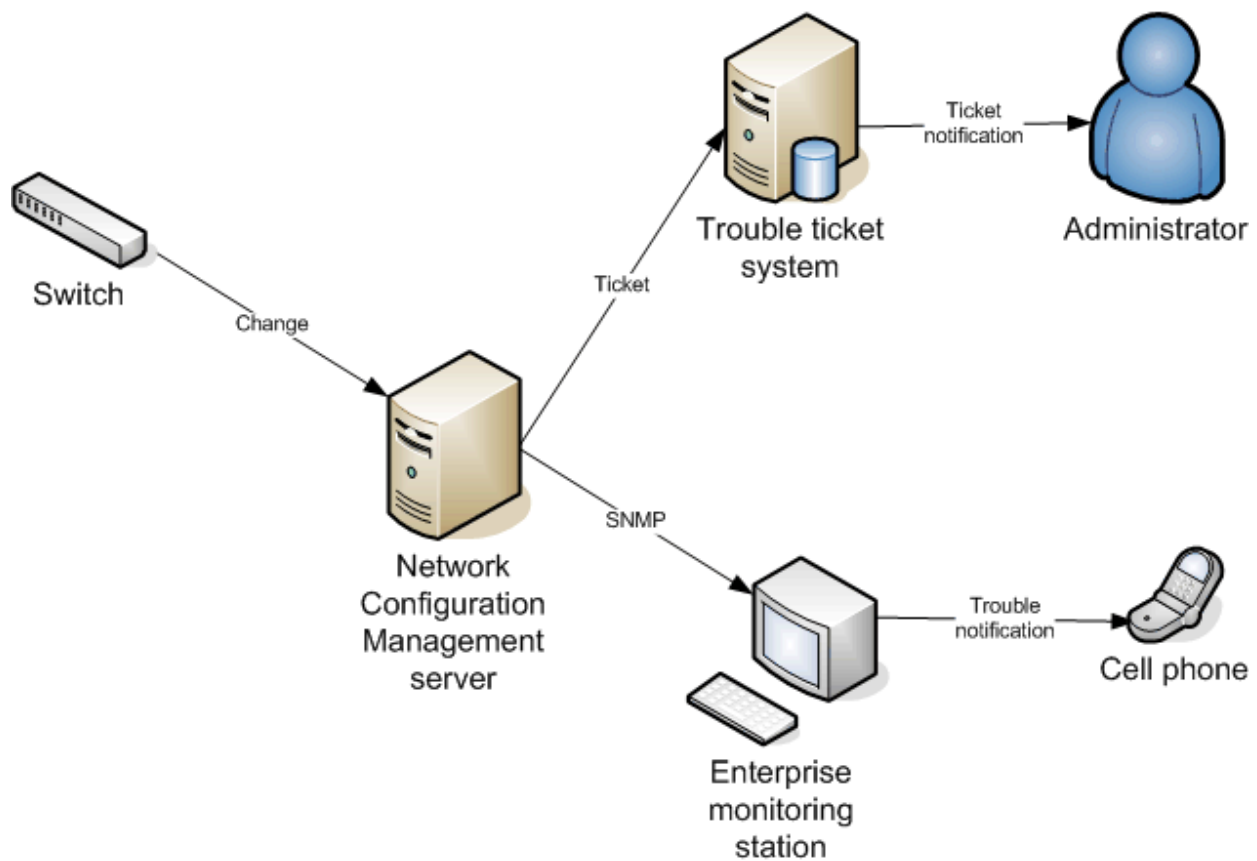
**Figure 3.5:** Using an external database for logging.

### **Change Notification**

Being notified of changes is at the heart of any good network configuration management solution. As previous chapters have reiterated multiple times, point-in-time audits are not useful in ensuring a continuously compliant environment. Going out of compliance for 5 minutes opens the possibility for a failure to meet your legal obligations. Being immediately notified of out-of-compliance changes allows your staff to react more quickly to bring the environment back into compliance.

The change notification capabilities of your solution must be flexible. Email is commonly supported, but the ability to support pagers (whether through direct-dial or email) and cellular phones (through Short Message Service—SMS) might be important to you for 24-hour, real-time notifications. Notifications are an immediate signal that something is wrong (typically, you'll only want to receive notifications for changes made outside your change management workflow), and immediate action is necessary. Thus, it is important that the notification get through to the right individuals as quickly as possible.

Change notification might also come in the form of integration with a Help desk system or via SNMP trap to an enterprise monitoring console such as HP OpenView. Figure 3.6 shows how a network configuration management solution might open a Help desk trouble ticket or send an SNMP trap to a monitoring station when an unexpected device configuration change is discovered. Solutions that can integrate their notifications into your organization's existing trouble-management systems will create less administrative overhead and allow your technical resources to respond more smoothly and consistently to unexpected or unauthorized changes.



**Figure 3.6: Integrating network configuration change notifications with your existing notification infrastructure.**

Some network configuration management solutions offer higher levels of integration with enterprise frameworks from companies such as Microsoft, IBM, and HP. This integration allows the solution's capabilities and services to become a part of your overall enterprise management strategy, rather than being a standalone solution that must be monitored and managed individually. If you already have an enterprise management framework, look for a solution that integrates with it.

### **Automatic Discovery**

Solutions that allow you to manually add devices to the roster of managed devices are fine, but solutions that can automatically *discover* devices are better. Why? You're likely to forget about at least one or two devices, and automatic discovery will ensure that all devices are included.

Automatic discover should be run on a regular basis—daily or even hourly, depending on your environment. This schedule allows the system to automatically discover devices that might have been added to the network without authorization. For example, the addition of unauthorized wireless access points is one of the biggest security concerns in any organization. By detecting the presence of these devices automatically, a network configuration management solution can alert you to devices not under its control and allow administrators to take immediate corrective action.

### **Dynamic Grouping**

Some solutions offer management by group. For example, after defining a set of policies, you might apply those policies to all Cisco routers in your organization. Although you might want to manually create static groups—groups reflecting geographic location, for example—for ease of management, the solution should ideally offer some means of dynamic grouping based on an analysis of the devices' own configurations.

For example, you might define a group that includes all Cisco routers running a particular version of the Cisco IOS, then apply specific policies to that group to monitor and enforce configuration settings that are specific to that IOS version. Anytime a new device with that IOS version is added to the network, it is automatically included in the proper group, and your policies are applied. This dynamic grouping simplifies management by applying policies based on evidence—configuration settings, for example—rather than applying policies based on an administrator remembering to put a device into a particular group. Figure 3.6 shows how applying policies to dynamic groups can simplify what would otherwise be a complex management situation.

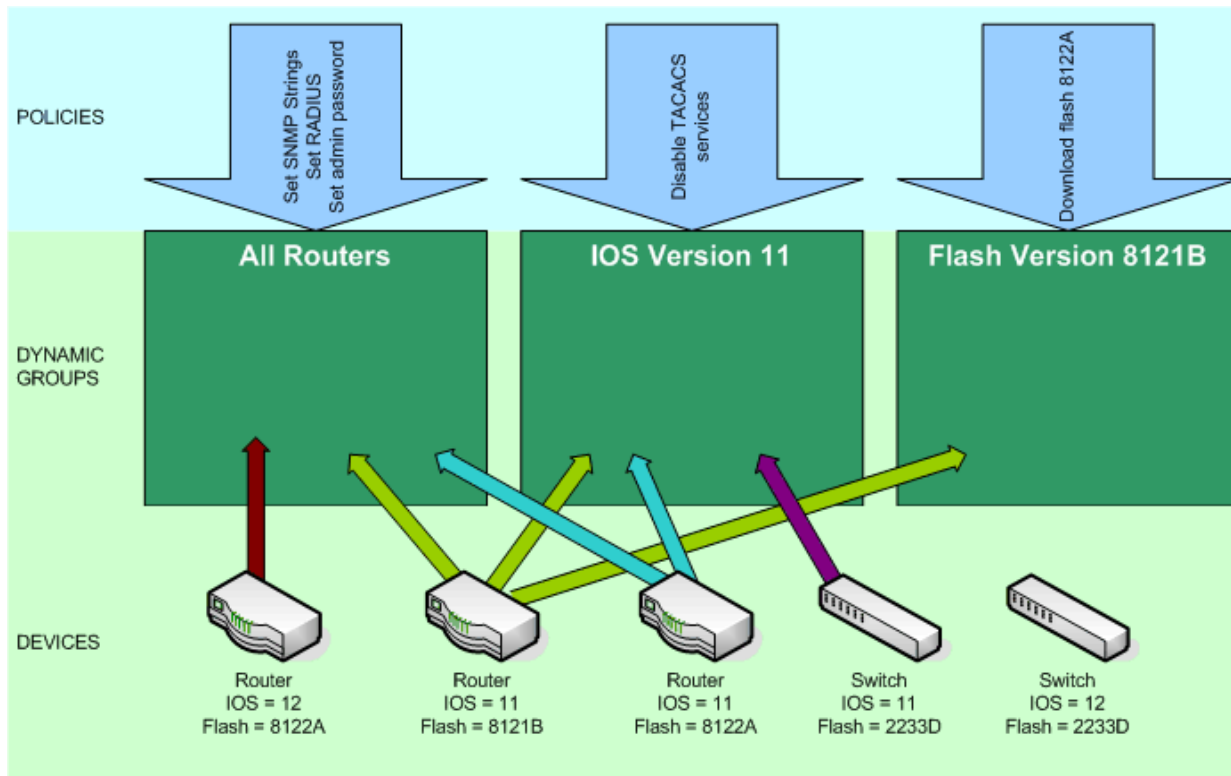
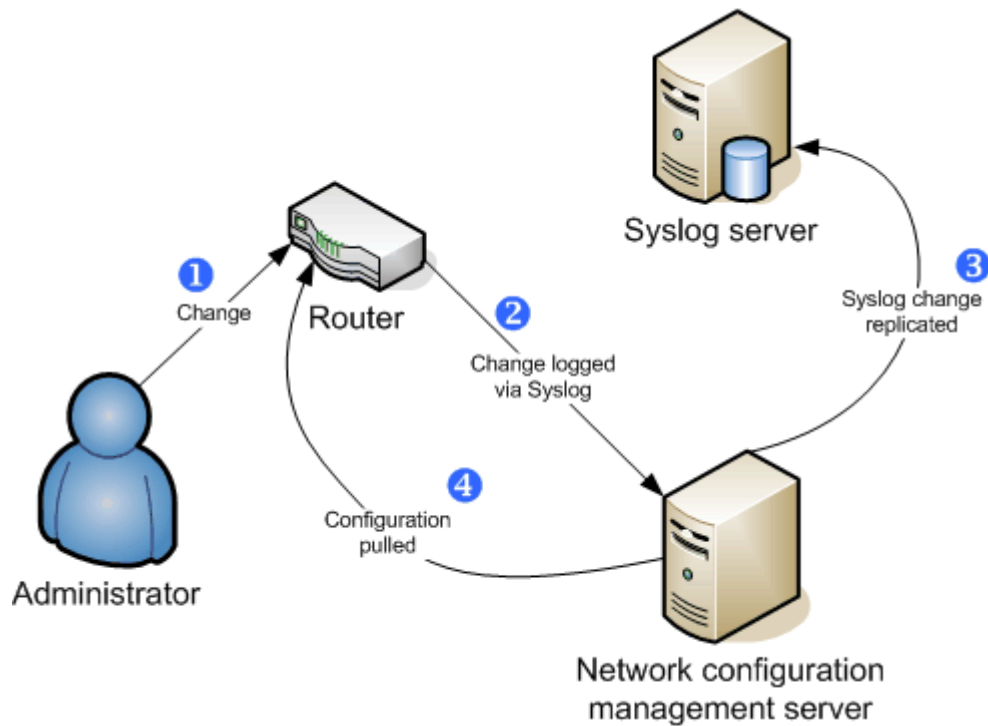


Figure 3.7: Dynamic groups can simplify complex policy application.

### Real-Time Monitoring

Configuration management solutions accomplish real-time monitoring through a variety of mechanisms. Some, as Figure 3.8 illustrates, act as a sort of Syslog proxy. When changes are made, properly configured devices report the change to their Syslog server, which is the configuration management solution. The solution might replicate the log entry to a real Syslog server for archiving but uses the event as a trigger to pull and analyze the device's new configuration.



**Figure 3.8: Using Syslog to receive change notifications and trigger a configuration analysis.**

This same technique can be used with RADIUS, TACACS, and SNMP. Regardless of the technology, the configuration management solution receives the trigger and pulls the device's configuration. The configuration can then be compared with any policies that are applied to the device and the proper configuration versions, and notifications to administrators can be generated.

Real-time monitoring is a crucial enabler for proper, real-time notification of configuration changes. This technique of using Syslog, RADIUS, TACACS, or SNMP as a trigger to check a device's configuration is more efficient than having the solution continually pull device configurations looking for changes. By waiting for an appropriate trigger, the solution knows that a change has occurred (or at least that an administrator did something that *might* have resulted in a change) and it can pull the device's configuration and take appropriate action.

### **Accountability**

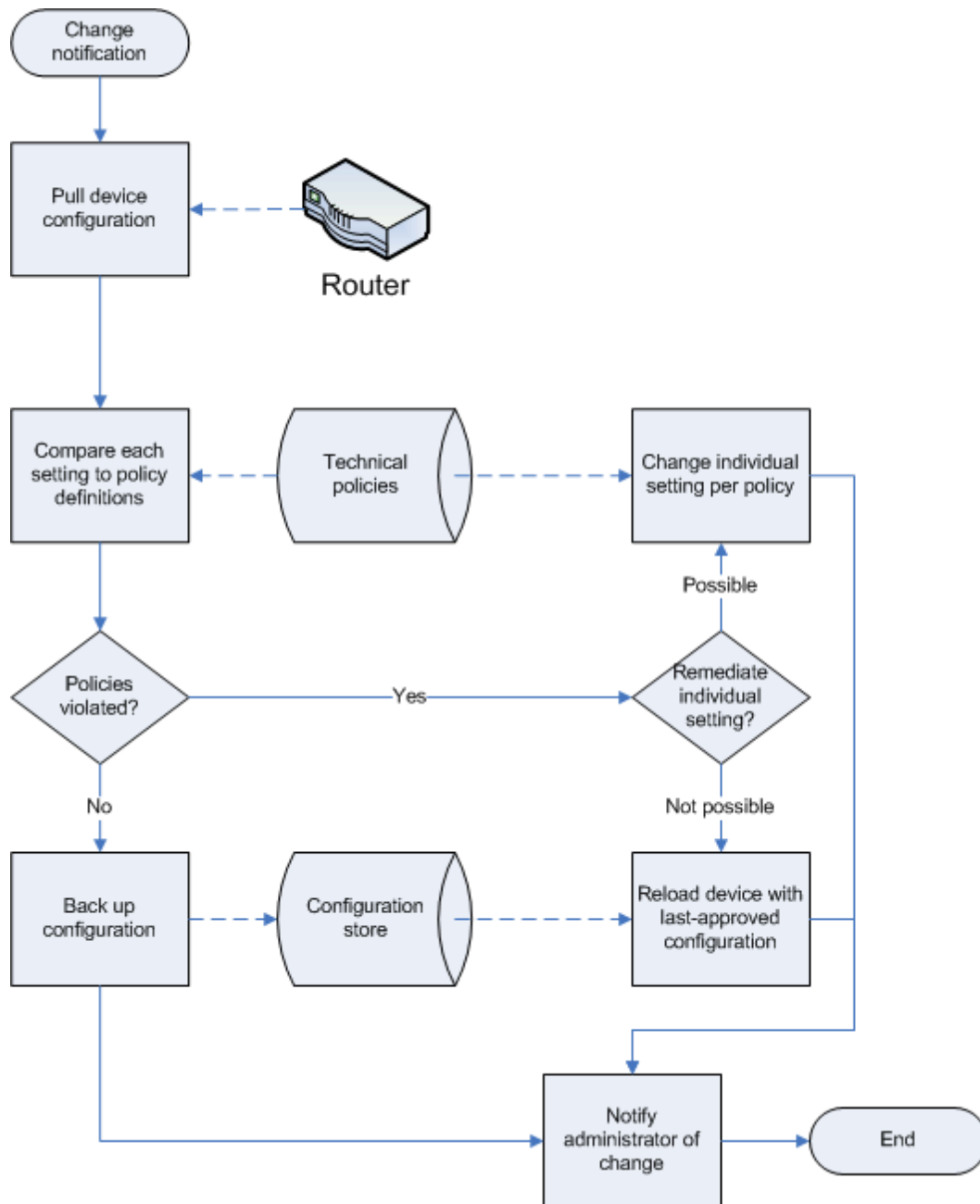
Accountability is a key compliance requirement for most organizations because the organization should always know when security-sensitive data (such as network device configurations) has changed and who changed it. By implementing technologies such as Syslog, TACACS, and RADIUS (or working with those technologies if they already exist in your environment), network configuration management solutions can provide the accountability you need for your compliance reports.

Many configuration management solution vendors are beginning to recognize the value of accountability—something many products have always offered—in a compliance environment, and are providing reports specific to compliance requirements.

The key with accountability, of course, is the *who* as well as the *what* of a change. Figuring out *what* changed in a device's configuration is usually easy but doesn't meet the requirements for accountability. Configure devices to use centralized authentication—such as RADIUS or TACACS—and to use logging mechanisms—such as RADIUS, TACACS, or Syslog—to log all access to the device. Doing so ensures that accounting information will be available in the log (either for a configuration management solution to receive directly or to pull from an existing logging server) and that the accounting information will contain useful identification information (provided through central authentication).

### **Enforcement**

One of the new trends in configuration management is enforcement. The theory is simple: Instead of merely alerting you to technical policy violations in device configurations, the solution can remediate the problem by reconfiguring the device to match the policy. This top-down management approach allows you to define policies that meet your requirements, then have the solution ensure that those are always in place. Figure 3.9 shows an example process.



**Figure 3.9: Basic process for automated enforcement.**

In this process, an administrator makes a change to a device. The configuration management solution receives notification of the change through some logging mechanism (perhaps SNMP) and pulls the device configuration. If none of the device’s configuration settings are contrary to policy, the solution might simply back up the new configuration and do nothing else. If some policy setting has been violated—perhaps the SNMP community string for the device was set to “public”—the solution might remediate the situation by either reconfiguring that one item or rolling back the entire device configuration to a previously approved version.

Initially, you will want enforcement to be limited to low-risk configuration settings such as SNMP community strings, RADIUS configurations, and so forth—items that, if incorrectly configured, won't cause your network to stop working. Eventually, however, your policy configurations should mature to the point at which automated remediation is possible for any configuration setting for which you can write a policy so that your network will never be out of compliance—even when unauthorized changes are made—for more than a few moments. At that point, you stop managing configurations and instead start managing policies. When a new router is added to your network, your configuration management solution can discover it, realize that it is out of compliance with your policies (as any new device would be), and enforce your policies—effectively putting much of the device's initial configuration into place.



This concept of managing via policy and having systems that can automatically configure or reconfigure resources to comply with policies is a core component of the Microsoft Dynamic Systems Initiative, HP Adaptive Enterprise, IBM OnDemand, and other similar initiatives in the IT industry.

### ***Rule and Policy Definitions***

Solutions should allow you to define granular rules for managing your devices. These rules should, whenever possible, affect only a single configuration item. This configuration allows the rules to be applied to multiple different devices. For example, a rule regarding SNMP community string configuration can apply to almost any type of network device. Rules are the building blocks from which technical policies are created.

Policies should therefore consist of one or more rules, and a policy should be able to incorporate any rule you have defined. This methodology allows you to create a large pool of configuration rules, then choose rules from that pool to create policies to apply to different types of devices. Ideally, technical policies should map one-to-one to your business-level policies, creating a strong relationship between business requirements (including those related to compliance) and the implementation of those requirements.


Top-down management via policy is definitely the wave of the future. As networks become more complex, dealing with individual device configurations becomes less efficient and less consistent. By defining technical policies, then having automated solutions that implement and enforce those policies, you can configure new devices more quickly and consistently, enforce configurations on existing devices more efficiently and consistently, and, in general, maintain your environment with less overhead and fewer mistakes. Configuration stops being a manual task performed by overworked administrators; instead, configuration becomes the automated response to policy changes, allowing administrators to simply define policies that govern how the network will be configured.

## Update Capabilities

Having the proper software on your network devices is so crucial to maintaining their security and functionality that a good configuration management solution should offer the ability to automatically deploy approved updates to your devices whenever a device is detected for which an update is available (and approved). You should never have to think about which devices *need* an update; the solution should automate that process. Instead, you simply define a policy: All devices of a certain description must be running this level of software. The solution should then implement that policy, analyzing device configurations to determine which meet your criteria, then deploying the update.

Contrast this setup to manual, point-in-time update deployment, through which you might miss devices, fail to properly deploy the update to each device, and so forth. Manual deployment also fails to consider new devices that might come out of the box with an older software version; automated deployment, in contrast, will immediately detect the new device, realize it doesn't comply with the latest-version policy, and fix it.

The solution must also provide the ability to deploy updates to a limited number of devices for testing. Updates should *always* be a part of your overall configuration management process, which includes reviewing the update for potential problems, deploying the update to a test environment and testing it, and so forth. Updates—no matter how critical—should never be deployed outside of your configuration management process. Very critical updates may be given an expedited path through that process, of course; placing priority on testing the update over working with other planned changes, for example, is a perfectly acceptable management technique. However, it's never acceptable to deploy a change of any kind—including an update—without testing it thoroughly and managing it through your existing configuration management process.

 Your configuration management process will have other valuable contributions to update deployment as well, including a step for backing up affected devices prior to deployment, post-deployment testing and verification, rollback in case of a problem, updating of environment documentation, and so forth.

## Solution Security

The security of your configuration management solution cannot be overlooked. These solutions store the complete configurations of every device on your network—they are a treasure trove for an attacker who wants to determine how your network is set up and how it works. Whatever solution you select, its database must be highly secured, and even encrypted, to help protect against unauthorized disclosure of this sensitive information. The solution should authenticate all access to configuration data, change management, and so forth (ideally, authentication should be through some centralized directory such as RADIUS or an enterprise directory such as Novell eDirectory, Microsoft Active Directory—AD, and so forth). All access to the solution should be logged for auditing purposes, and the log must include the identity of all individuals accessing the system in order to provide compliance-level accountability. If the solution uses a back-end data store (such as a SQL Server system), it should either automatically configure the data store with appropriate security and/or encryption, or provide you with detailed instructions about how to do so.

## Summary

Compliance management for network infrastructures can be complicated but doesn't have to be. The right solution can provide a high degree of automation for compliance management, even in highly diverse environments that employ devices from several manufacturers. Top-down management—defining policies that are automatically monitored or even implemented and enforced—provides a layer of management abstraction in an increasingly complex field, helping to improve efficiency and consistency as well as productivity and reliability. Combined with a solid change management process, you can reduce downtime, improve compliance, and reduce the cost of managing your network.

---

## Chapter 4: Network Compliance Best Practices and Methodologies

Compliance management at the network infrastructure level can be complicated. Combining difficult-to-understand legal requirements with detailed, complex technologies often results in confusion, frustration, and difficulty. Many organizations do the best job they can, relying on simple point-in-time audits to ensure compliance. These companies are then surprised when their networks are able to quickly go out of compliance, often without anyone taking notice.

As I've discussed in the previous chapters, however, compliance doesn't have to be complicated. By managing compliance requirements as you would any other type of business policy, and by implementing tools that can automate compliance and configuration management, maintaining a compliant network can be straightforward. Another way to simplify compliance management is to implement best practices and sound methodologies for managing your network, which is what this chapter is all about.

### The ITIL Framework

The Information Technology Information Library (ITIL) was developed by the Office of Government Commerce (OGC), a branch of the British government. ITIL is a vast compilation of best practices and procedures for managing an IT organization. Although this library doesn't specifically address compliance, ITIL offers plenty of advice for change management, which is a key part of compliance.

All compliance-related legislation—HIPAA, the Sarbanes-Oxley Act, 21 CFR, and so on—boils down to two requirements as far as IT is concerned:

- Getting your environment in a condition that is both secure and accountable
- Keeping your environment in that condition

There is actually a lot of abstraction between most legislation and your network infrastructure. For example, the Sarbanes-Oxley Act doesn't offer specific regulations about how routers should be configured. The act is concerned only with the security of confidential information. Of course, your network is the primary means for transmitting that confidential information, so your network must be configured to prevent unauthorized disclosure of that information. This configuration is not difficult to realize, and most organizations have their networks set up that way to begin with, thus achieving an important part of compliance. The difficulty comes in ensuring that the network *stays* that way—firewalls aren't misconfigured, routers are programmed to transmit data off the network, and so forth. The Sarbanes-Oxley Act requirements for accountability are almost entirely reactive. Knowing *who* made a change is interesting for punishment purposes, but the fact is the change *was* made. If the change took you out of compliance, it is useful to know what happened and who did it, but it doesn't change the fact that you did go out of compliance.

The trick, then, is to eliminate changes that will take you out of compliance. In other words, change management is crucial to compliance management. Change management is hardly a new concept—preventing unauthorized, untested changes is an efficient way to reduce downtime, reduce troubleshooting efforts, and generally improve network operations. Change management also happens to be an effective way to handle network-level compliance management. The idea is to get your network into a compliant state, then closely manage changes to ensure that you remain compliant—a process that is supported by ITIL.

ITIL defines a model change management process that is, in theory, effective for any type of change management effort: networks, software development, and so on. Figure 4.1 illustrates an example, simplified process.

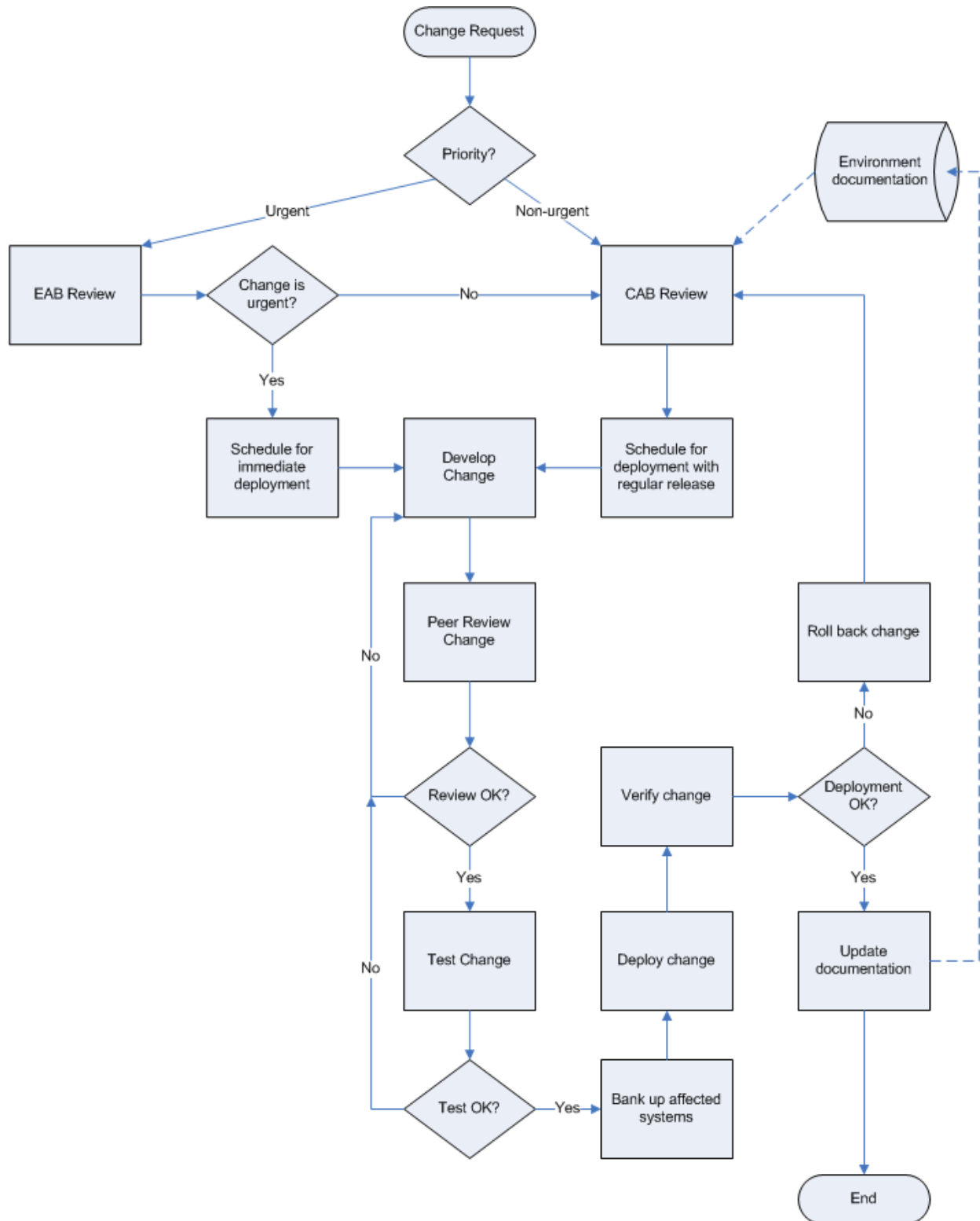


Figure 4.1: Simplified ITIL-inspired change management process.

Everything starts with a change request. Requests can come from a number of sources; they might originate from a user, a Help desk ticket, or as part of a bigger project to expand or redefine your network. Regardless of where the request comes from or what it involves, it is treated the same. First, it is prioritized, often by the person who submitted the change to begin with (for example, an administrator). Lower-priority changes are considered on a regular basis by what ITIL calls the Change Advisory Board (CAB), a panel of management and senior technical professionals. Higher-priority changes don't need to wait for the regular CAB meeting; these types of changes are sent through an Executive Action Board (EAB), which handles high-priority concerns. The EAB can, of course, decide that a change is not an emergency and relegate it to the CAB.

Each of these panels' jobs is to decide which changes will be approved and when the changes will be deployed. The CAB generally seeks to bundle changes into releases, making several changes at once to the production environment. As a result of the higher-priority nature of the changes they review, the EAB generally approves changes for more immediate, independent deployment.

#### **Singles or Batches: Risks of Making Changes**

The IT industry often takes a "make one change at a time" approach for reconfiguring networks, based on the theory that if something goes wrong, the problem will be easier to fix if a change is made independently rather than in a batch with a bunch of other changes.

A different approach is to thoroughly test and pilot changes prior to making them, then deploy them in a batch because you know that they won't cause problems. Testing and piloting are often ignored at the network-configuration level, but they are crucial steps. Deploying untested changes is simply foolish, even if you know you can quickly undo the change in case a problem occurs. Problems, in fact, might not rear their heads for days or weeks, at which point other changes might have been deployed and long past the point where the original change can be easily identified as the trouble source.

Once a change has been approved and scheduled for deployment, the change is developed by a technical professional. The change is then tested and peer reviewed for accuracy and potential problems, and corrected if necessary. Once tested and approved, the change is placed into the queue for deployment according to the schedule set by the CAB or EAB. The primary purpose of the CAB/EAB is to focus on the overall network environment, bundling changes to improve the network, reduce risk, and maintain a compliant state. The CAB can, for example, identify changes that might have an adverse affect on compliance, then spell out specific areas of the change to be tested or reviewed to ensure that those areas don't have a negative effect on the organization's compliance. By managing change from the top down in this fashion, compliance can be more easily maintained.

Automated change management tools can help facilitate and enforce this workflow. For example, tools can be used to automatically deploy approved changes, detect and undo unapproved changes, and prevent unapproved or unreviewed changes from being accidentally deployed into the production network.

A solid change management process can help establish a foundation for your entire compliance management efforts. It provides a framework for changes to be reviewed against your business policies—policies that should incorporate any compliance requirements, as the next few sections explore.

## Network Compliance Management

Many companies struggle with their compliance efforts mainly because they are treating compliance as an independent entity rather than as a part of their overall business. In the rush to become compliant, and in the effort to determine exactly what that means from an IT point of view, the primary driver for the network becomes compliance rather than business, which can diminish productivity and cause considerable frustration. Companies need to adopt a different management model—one that embraces compliance as a part of doing business and creates a set of business policies that incorporate both compliance requirements and what the business needs to function and thrive.

### **Assemble Your Business Policies**

Start by creating a set of written policies that cover all of the business' needs. Be selfish here: Don't try to factor in any requirement that doesn't directly benefit the business in some fashion. This set of policies is the ideal set—the items you would put in place if there were no regulations or legislation to the contrary and if the only thing that mattered is the business.

Avoid drafting policies that have any kind of technical feel to them. Technology is merely a tool; the goal at this point is not to dictate how or what tools will be used but to codify what the business requires in order to survive and grow. For example, a policy statement such as *Customers will be able to access their financial data over the Web at all times* is too technology-centric; bring the statement up a level and simply state *Customers will be able to access their financial data at all times*. This broader policy statement will drive service level targets not only for a customer service Web site but also a call center and any other means through which a customer might access their information.

Also try to avoid security- or compliance-specific policies at this point. For example, avoid policy statements such as *Customer data will be protected and all access to customer data will be recorded*. This goal doesn't really benefit the business. A more business-level goal along the same lines might be something like *Customers will feel comfortable entrusting their confidential data to our company*. This broader statement benefits the business because it drives customer satisfaction; it implies more detailed considerations such as security and accountability, but focuses entirely on the business benefit of those items.

This point in the policy development process is a good time to flowchart your major business processes, if you haven't done so already. Focus on those business processes that affect or rely on the network. For example, consider the somewhat generic flowchart in Figure 4.1, which covers change management for the network configuration. You might update that flowchart to look more like the one that Figure 4.2 shows, which is more organization-specific, adds a focus on business needs, and is entirely network-centric.

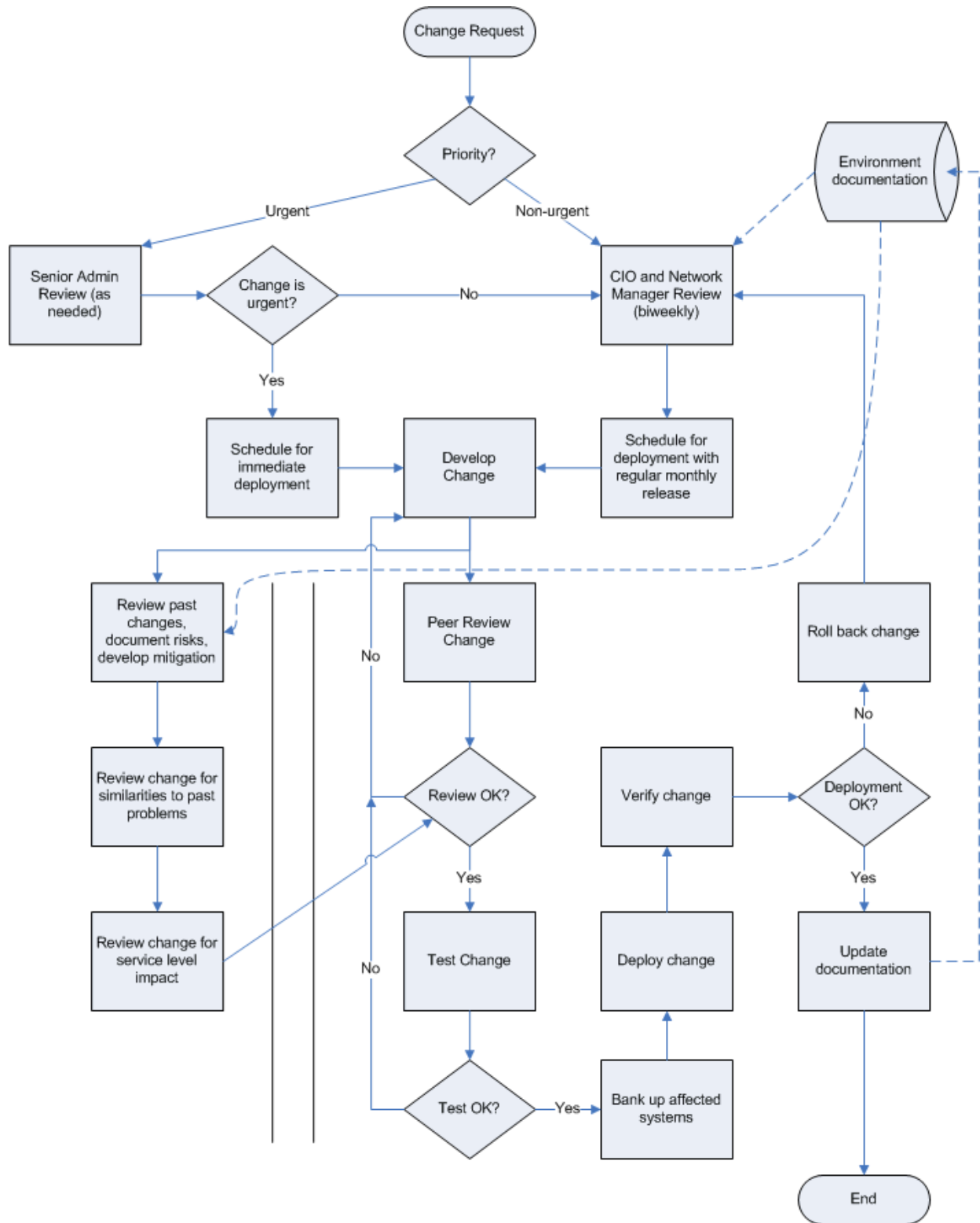


Figure 4.2: Adding business-level concerns to a process flowchart.

This revised flowchart includes an independent parallel review of proposed changes and developed changes to specifically focus on business-level impact (service levels), as well as a “learn from our mistakes” review through which another administrator or technical professional reviews past changes to find any similarities to the proposed change so that any problems that occurred in the past can be specifically considered and avoided this time. The reviewing entities (EAB and CAB) have been replaced with entities specific to this organization, and some basic service levels around their reviews (biweekly or on demand) noted.

### **Integrate Legal Requirements**

Next, modify your policies and process flowcharts to accommodate any legal requirements that apply to your organization. For example, you might modify processes to ensure that actions are being properly documented and logged, that accountability is considered, and so forth. You’re not documenting your current processes at this point; you’re documenting what you *want* your processes and policies to look like in a perfect, compliant world. At this point, settle any conflicts between business and legal compliance requirements so that the technical professionals who implement the technology to meet these policies and processes can be assured that the implementation will meet the business and legal compliance requirements.

Again, keep policy statements non-technical. A statement such as *Files containing customer information must be secured by using file security and encryption* is too specific; modify the statement to *Customer data must be secured so that only authorized individuals can view or change it*. This broader policy applies to not only electronic data but also hardcopy files, which is an area in which many organizations’ elaborate electronic security measures can be easily circumvented. Don’t focus on tools such as paper or computer files; focus on the requirement, which is to keep data confidential.

Policy conflicts might occur at this point. For example, a business policy stating *Customers must be able to access their financial information at all times* may conflict with the legal requirement *All access to customer data must be logged for auditing purposes*. What if a customer wants to access their data and the logging system is unavailable? To address this conflict, the policy statements might be modified to create a statement that reads *All access to customer data must be logged for auditing purposes; customers must be able to access their financial information at all times provided that such access can be logged at the time*. This clear statement resolves the potential conflict in favor of the legal requirement for logging rather than in favor of the business requirement for continuous access at all costs. Through this statement, technical professionals implementing this policy will know that it is okay if customers can’t access their data when logging services are offline (and might be able to better understand the need for a highly fault-tolerant logging system). Similarly, facilities management personnel will know that hardcopy files can remain locked if a suitable log book or other auditing mechanism isn’t available to log access to the files.

At this point, review your network-related business processes and add annotations that provide legal compliance. For example, the flowchart in Figure 4.2 provides business-level requirements for a network configuration change management process but doesn’t provide the accountability that many organizations now face as a legal requirement. The flowchart in Figure 4.3 resolves this shortcoming by adding annotations that indicate where logging and auditing must occur.

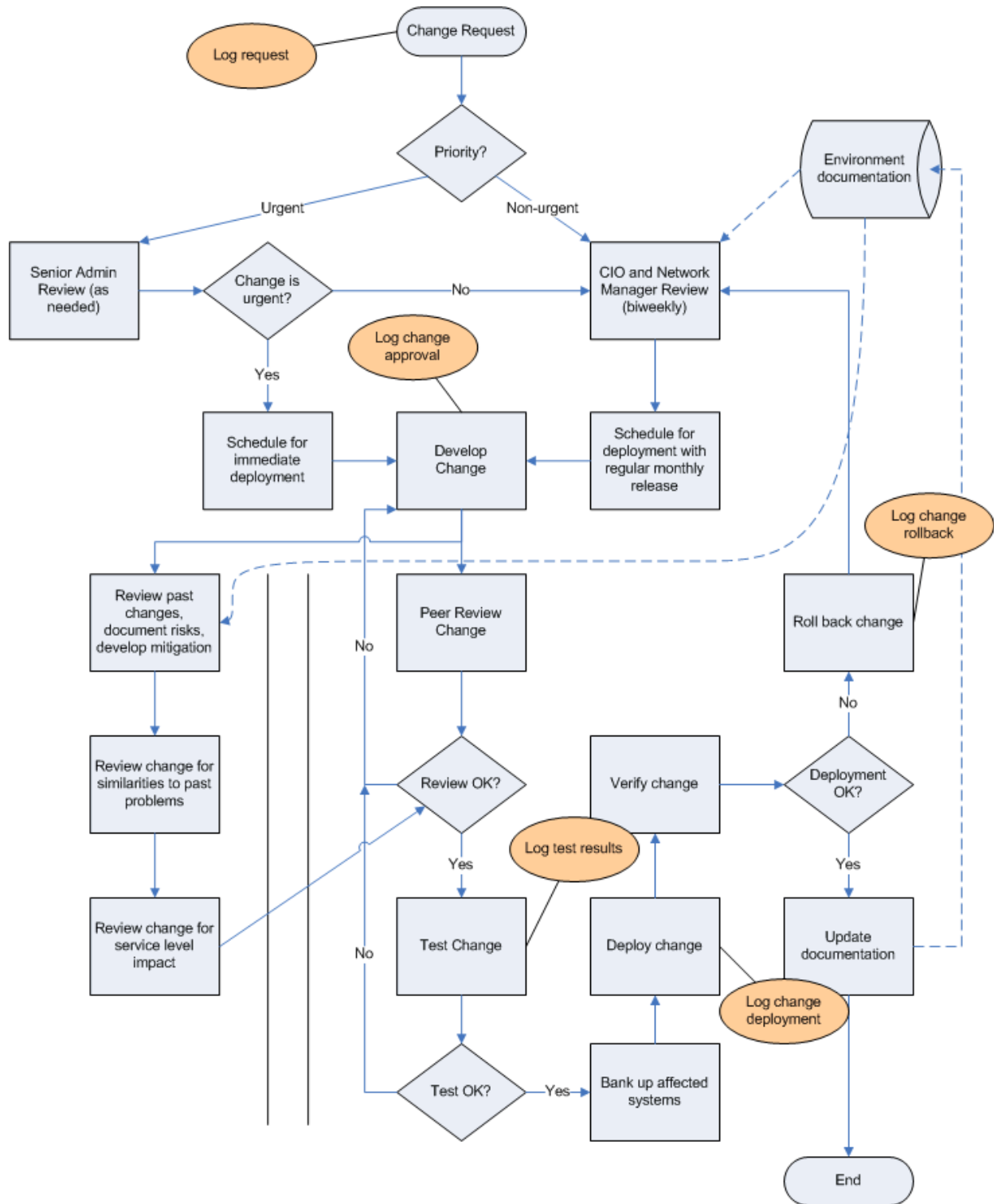


Figure 4.3: Adding legal requirements to your management processes.

The goal is to create *one* set of processes and policies that not only accommodate the business' requirements but also meet any legal requirements to which the organization is obligated to adhere. This task takes more effort on the part of management because existing business policies and requirements might not be well-documented and the actual impact of legal requirements might not be fully understood. If necessary, bring in consultants to help you sort through the business and legal requirements and shape them into policies. Avoid hiring consultants who promise to simply “make everything compliant” without a complete understanding of your business; such consultants can do harm to the business, and without a single set of business-and-legal-requirements policies, your staff will be less able to efficiently maintain the infrastructure that the consultant sets up for you.

### **Layer in Security**

Security is something that affects everything you do; a fact that will be reflected in your normal business policies in such statements as *Customers will feel comfortable entrusting their confidential data to our company*. Legal requirements often take a security focus, as well, and policy statements such as *All access to customer data must be logged for auditing purposes; customers must be able to access their financial information at all times provided that such access can be logged at the time* will reflect that. But security is important enough that you should take one final pass through your policies to add in any security-specific details that might have been left out to that point. For example, you might want to further amend statements such as the last one to read *All access to customer data must be logged for auditing purposes; customers must be able to access their financial information at all times, provided that such access can be logged at the time and that such access can be protected from eavesdropping or accidental disclosure*. This modification is significant: Customer access through means such as the Web will now need to be encrypted, and faxing customer information may now be totally out of the question because that technology doesn't provide much in the way of guaranteed confidentiality. These needs could create a potential conflict with business requirements; if so, you will need to review the two sets of requirements to decide where to compromise. For example, you might decide that certain *kinds* of customer information can be disclosed through means that can't guarantee confidentiality, allowing you to fax a mortgage payoff statement, for example, but not to fax complete account statements.

In addition, examine your business processes (in this case, I'll continue to focus on those that affect network management) to layer in security requirements. At this point, an understanding of the underlying technologies will obviously be helpful in determining appropriate levels of security. In Figure 4.4, I've added security-specific annotations to key portions of the network change management process. You'll notice in the annotations that I'm assuming some sort of role-based security will exist, allowing me to assign individual technical professionals to roles such as Change Developer, Change Reviewer, Change Tester, Change Deployer, and so forth; role-based security is one of the benefits some configuration management software tools provide to make network configuration security easier to manage.

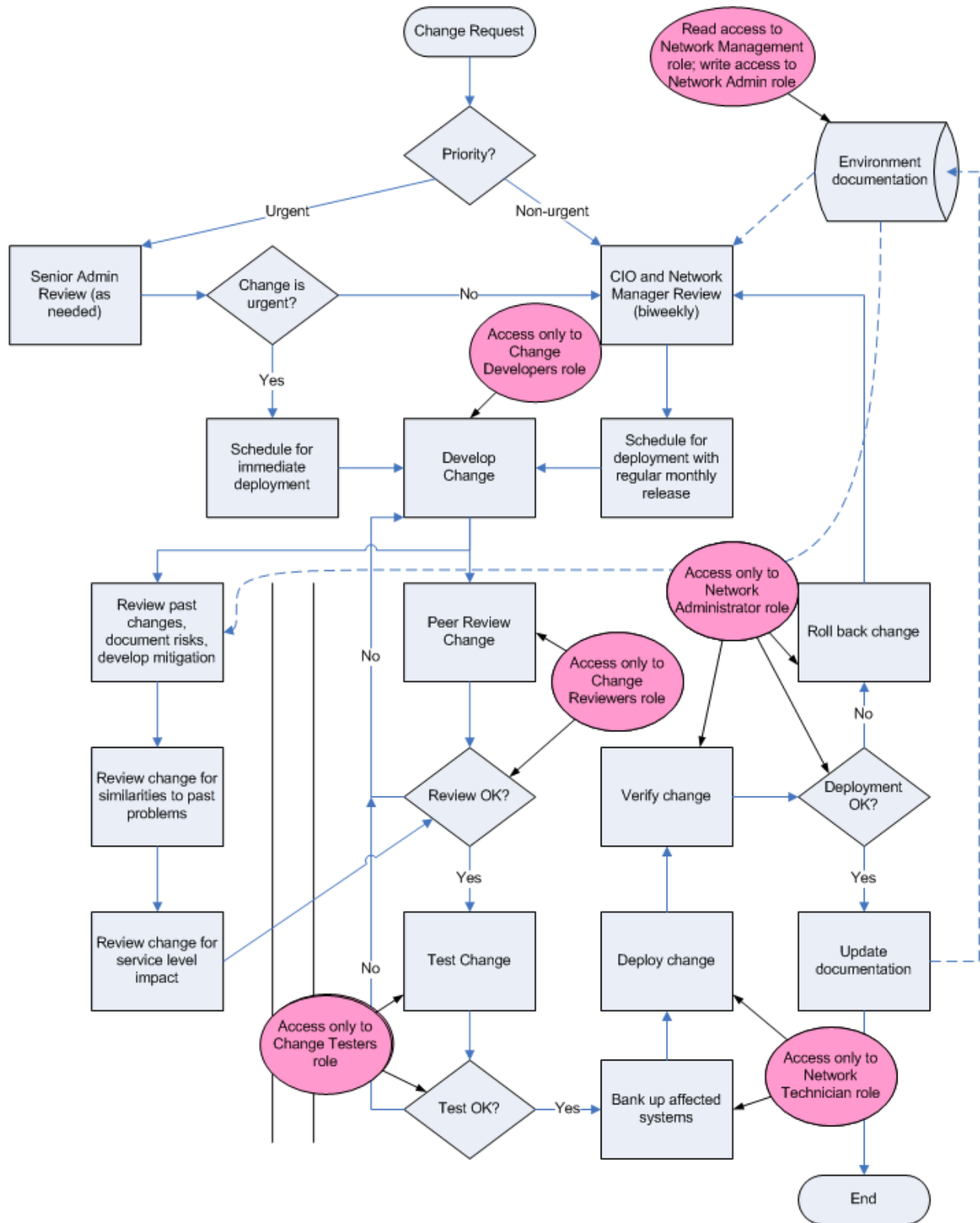


Figure 4.4: Adding security-specific concerns to a business process.

This last step helps to document any specific security requirements or configurations. It can also make the tool-selection process easier if you're shopping for configuration management tools; with your security needs more firmly defined, you will be able to look for a tool that can implement the security you want.

### **Create Your Final Business Policies**

Your final business policies are a combination of your business requirements, compliance requirements, and legal requirements. Statements such as *All access to customer data must be logged for auditing purposes; customers must be able to access their financial information at all times, provided that such access can be logged at the time and that such access can be protected from eavesdropping or accidental disclosure* are effective business policies because they encompass the needs and concerns of the business. By remaining technology-agnostic, these policies can be broadly applied across the organization to information systems, facilities, customer-access systems, and so on. These single, comprehensive policies can serve as a sort of organizational Constitution, defining minimum requirements and concerns and resolving any conflicts that might exist between different management concerns (such as business needs and compliance requirements).

Your final business policies should be written (or published electronically, of course), and made available to the entire organization. These policies will drive the development of everything in the business, and will become the guiding hand for your network compliance management efforts.

### **Applying Management Policies**

Once your policies are in place, you need to take stock of your network:

- What have you got that needs to be managed?
- What specific things will you have to configure, and how difficult will they be to manage?
- What kinds of tools might be available to help make the job easier?

A thorough inventory of what you have and what you need to do will help get you into your compliance management faster and more effectively.

### **Inventorying Your Network**

Inventorying your network can be a difficult task. Many networks contain so many devices that it's difficult to remember them all, and documentation quickly gets outdated if careful change management practices aren't followed. It is strongly recommend that you find a tool that can do automatic network discovery for you. These tools start by querying one computer's local subnet and default gateway for devices and routes; the tools then follow the routes to query additional subnets and routers until they have eventually queried every IP address on your network and discovered every available device. This method is the most effective way to inventory; it is also a useful practice to perform as a periodic security check to make sure unauthorized or unknown devices aren't showing up on your network.

---

## ***Inventorying Your Needs***

Once you know what you have, you can start to evaluate your specific network management needs:

- Do you need auditing?
- Do you need reporting?
- Will you need something that can work with multiple vendors' equipment, or are you in one of the very few companies that have a completely homogenous network infrastructure?
- What sort of compliance reporting will you need?

The discussion in Chapter 3 should help you identify needs that exist in your environment. You can then move forward and begin evaluating tools that meet those needs.

## **The Right Tool for the Right Job**

As I've already mentioned several times, the right tool can make network configuration and compliance management much easier. Many tools exist to help with various aspects of configuration management, and many are beginning to offer compliance-specific features to help you in that regard, too. You will need to evaluate several tools and grade them on their capabilities, then select the tools that best match your business processes.

## ***Evaluating Management Tools***

The previous chapter provided a shopping list for network configuration and compliance management tools; use that list to help further refine your business needs, if necessary, and evaluate the tools you will need. I prefer to construct a sort of score card, filling it in with a score of 1 (poor) to 5 (excellent) for each feature that is important to the organization. Keeping your needs in mind, assign a score of 1 (nice to have) to 3 (absolutely necessary) to each need; multiply each product's scores by your need scores for a weighted score that shows how each product meets your most important requirements. Figure 4.5 shows a portion of a sample evaluation.

Feature by Feature Comparison

	NEED SCORE	Product A	Product A Weighted	Product B	Product B Weighted
Vendor-agnostic	2	5	10	5	10
Reporting	3	4	12	5	15
Logging/Auditing	3	4	12	4	12
Change notification	3	5	15	5	15
Auto-discovery	2	1	2	4	8
Dynamic grouping	1	1	1	3	3
Real-time monitoring	2	3	6	4	8
Accountability	2	4	8	4	8
Enforcement	3	1	3	4	12
Rules and Policies definitions	3	1	3	4	12

72

103

Figure 4.5: Evaluating tools that meet your needs.

### Matching Your Tools to Your Processes

Once you have selected a tool, or as a part of your evaluation process, consider specific features that map to and support your business processes. There is no point in purchasing tools that don't do what you need them to do, and you shouldn't have to make drastic changes to a well thought-out process just because your tools don't work that way. Tools should adapt, and they should work with whatever processes you have in place. Simply take the process flowchart and list annotations that indicate how a tool supports each bit of the process. Figure 4.6 shows an example; notice that some features—such as tracking change requests prior to them being approved—aren't provided by this particular tool; I'd need to provide that functionality elsewhere, perhaps through my Help desk ticket tracking system (which, as I've indicated, this tool can integrate with).

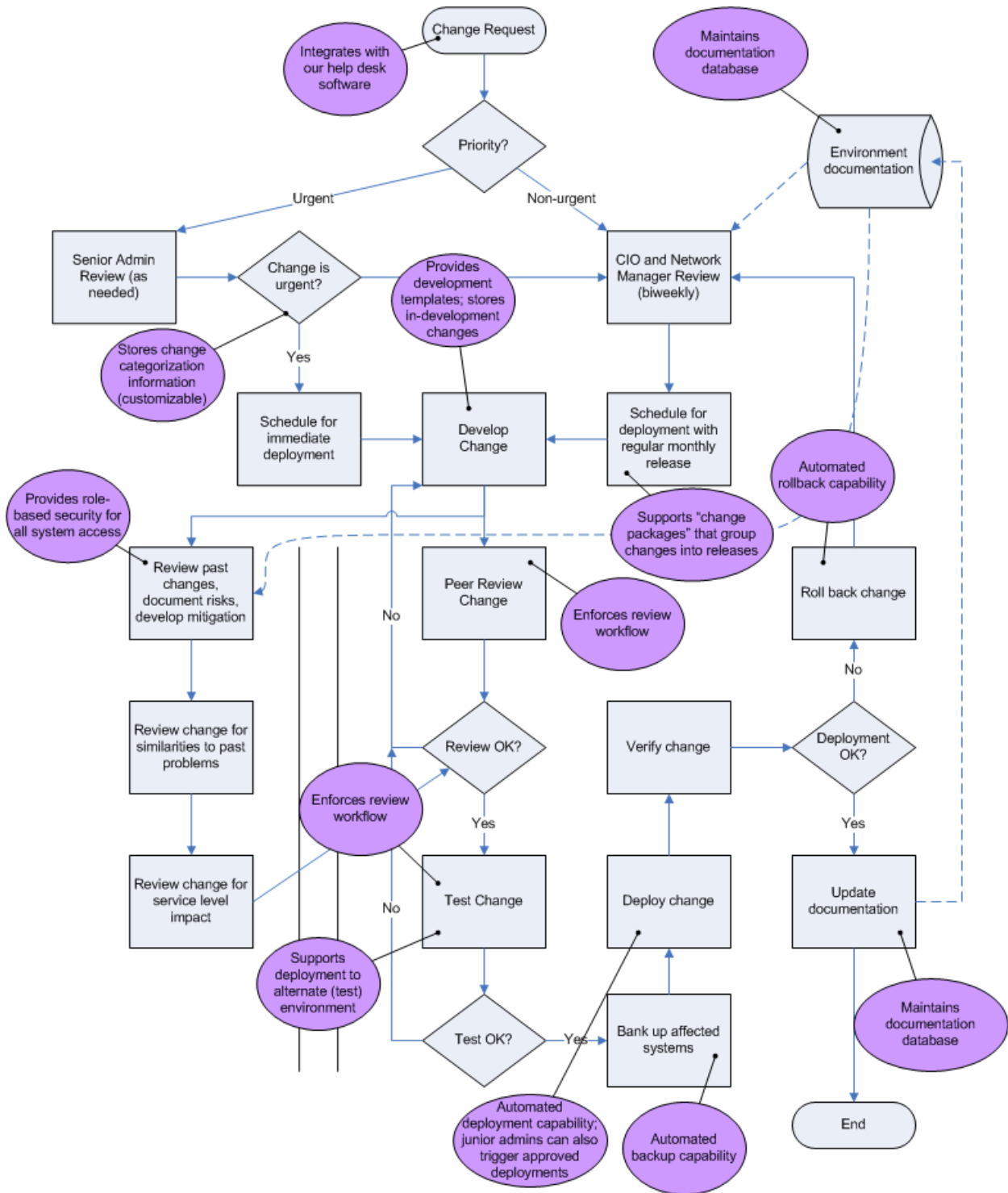


Figure 4.6: Mapping a configuration management tool to my processes.

At this point, start mapping tools to business policies. For example, if you have a policy that states that *All configuration changes made to systems that store or transport confidential data must be logged for auditing purposes*, you might make a note that a particular tool supports this policy by providing real-time monitoring of device changes, as well as logging any changes made inside or outside of the tool for auditing. The tool might even provide a report listing all recent device configuration changes, further supporting this business policy.

## “Do’s and Don’ts” for Network Compliance

The following list highlights tips that can help improve network compliance, along with some things that can make it vastly more complicated and expensive than it needs to be:

- **Do** treat compliance requirements like any other business requirement.
- **Do** create a single set of business policies that include both business and compliance requirements and are broad enough to drive all of your business practices, not just technology.
- **Do** invest in tools that can automate configuration and compliance management tasks.
- **Don’t** allow technical professionals to resolve conflicts between business requirements and compliance requirements.
- **Don’t** expect technical professionals to interpret legal requirements into technical ones; do so for them by incorporating the legal requirements into your business policies.
- **Do** create technical policies that map to your business policies and specify technical implementation details (rules) that comply with those business policies.
- **Do** adopt a policy-driven management style for your network management. Use tools that can monitor and enforce compliance with technical policies.
- **Don’t** always look only at tools that specifically target compliance; plenty of tools offer features that help deal with compliance, even if they aren’t specifically named that way.
- **Do** look for tools that are vendor-agnostic and that abstract vendor-specific configuration data into a uniform, generic format.
- **Do** look for solutions that have security built-in and offer a security model that supports your policies and processes.
- **Do** rely on consultants or service bureaus to help you determine how legal requirements apply to your network infrastructure.
- **Don’t** rely on consultant or service bureaus to do your compliance work for you; you need to have policies and people in place for long-term maintenance.

## “Do’s and Don’ts” for Network Security

In a similar vein, here are some do’s and don’ts for network security:

- **Don’t** treat security as an independent entity. Integrate security into all of your decisions, processes, and policies right from the start.
- **Do** make a final “security review” of processes, decisions, and policies to ensure that security-related considerations have not been overlooked.
- **Do** look for tools that offer the highest level of security possible, such as role-based security, data encryption, auditing capabilities, and workflow enforcement.
- **Do** rely on configuration management to avoid security problems.
- **Do** implement a peer review for proposed network changes, and include security concerns in that peer review.
- **Do** stay up-to-date on security information from equipment vendors, and install the latest patches or configuration changes as recommended.
- **Do** resolve compromises between security and business requirements at a management level.
- **Don’t** establish security policies that are technology- or medium-specific; establish companywide policies, then apply them to every aspect of the business, including technology.

## Summary

Hopefully, this guide has provided you with a useful overview of network configuration and compliance management. If you take only one thing away from this book, let it be this: Compliance management is no different from regular management; it’s just imposed by an outside authority. Treat it as you would any other business requirement, and make it a part of your everyday business practices, management processes, and business policies. Doing so will make compliance easier to achieve, easier to maintain, and much less likely to negatively impact your business. Investigate tools that can help ease some of the burden. Tools exist that can provide auditing, accountability, and robust, policy-based management for network devices. Network compliance management doesn’t need to be difficult, particularly with a consolidated set of business policies and the right tools.