

realtimepublishers.comtm

The Shortcut Guidetm To



Network Compliance and Security

AlterPoint

Don Jones

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

Copyright Statement

© 2005 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.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 Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.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.

Realtimepublishers.com and the Realtimepublishers 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 Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com

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.

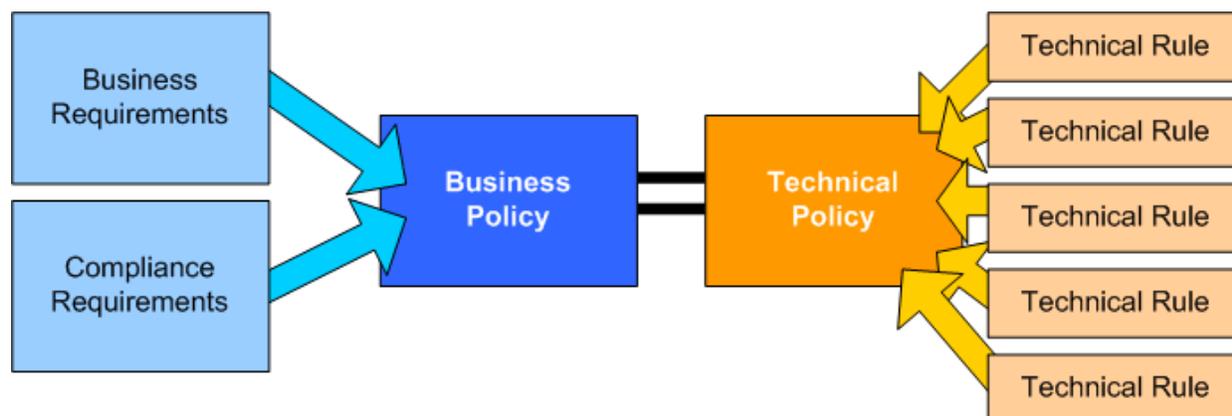


Figure 3.1: Mapping business policies to technical policies.

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.

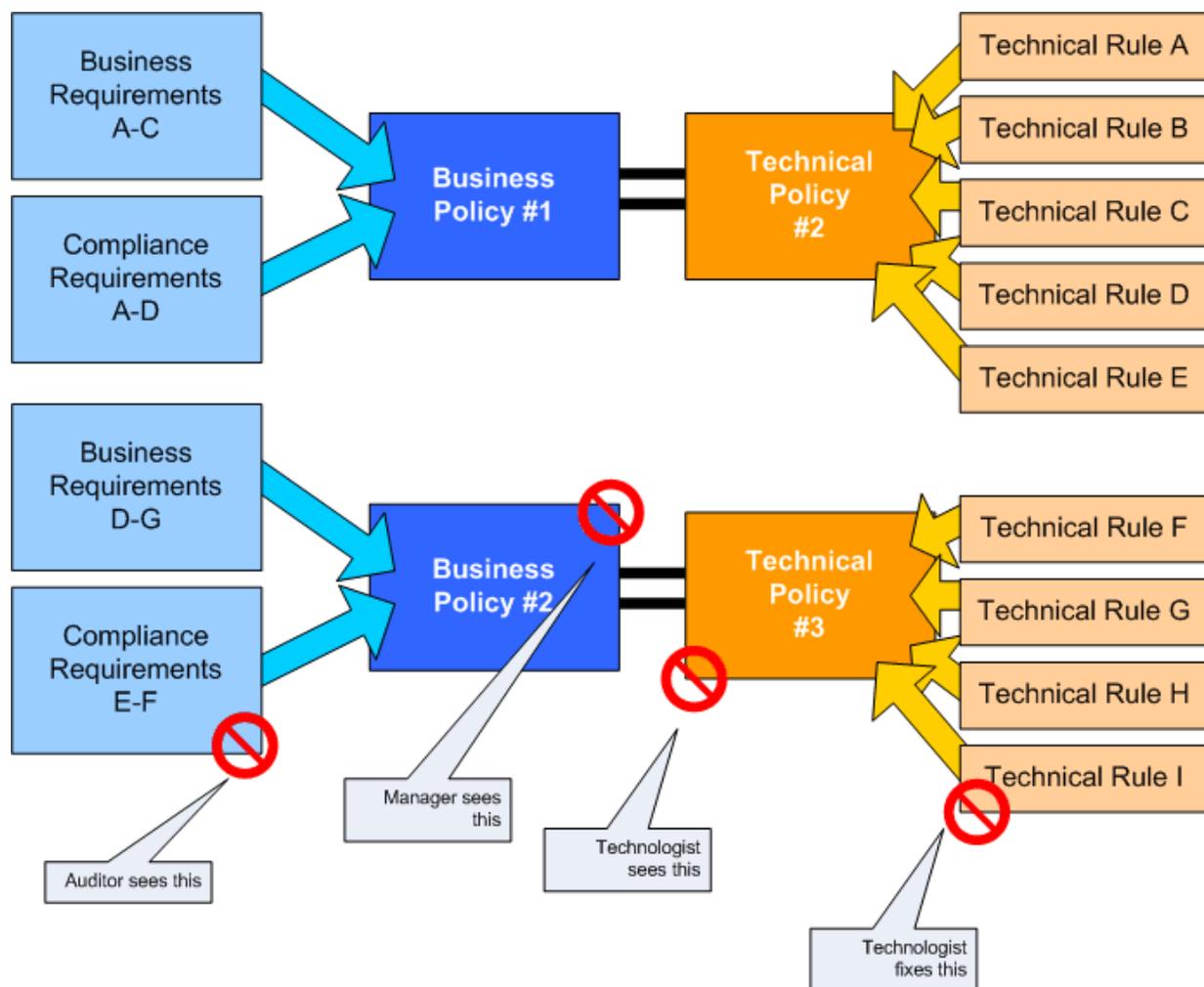


Figure 3.2: Creating mappings between business and technical policies creates more insight for each level of an organization.

 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.

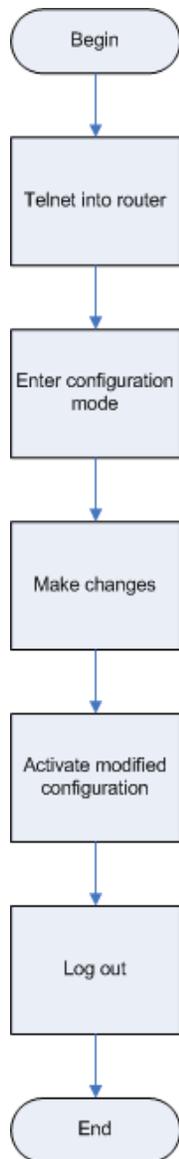


Figure 3.3: Pre-compliance router configuration process.

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.

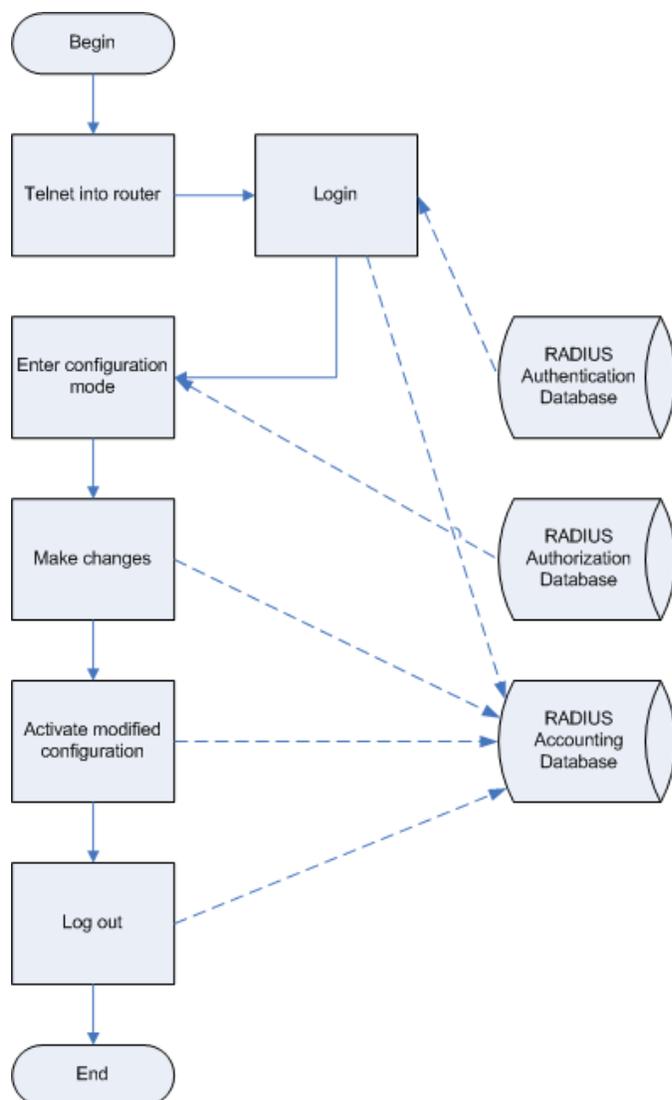


Figure 3.4: Post-compliance process shows additional detail.

The process in Figure 3.4 isn't necessarily different than the process that Figure 3.3 shows, the post-compliance chart simply explains the process in more detail. The original process (which Figure 3.3 shows) doesn't have any requirement for RADIUS, for example, and doesn't show accounting, authorization, or authentication in place. However, this lack of representation of these requirements doesn't mean that they don't exist, just that they weren't a documented part of the process.

Part of compliance is documenting the parts of your business processes that support compliance requirements; Figure 3.4 does so. This figure also makes it clear to technical professionals that these additional steps—and the inclusion of RADIUS for accounting, authorization, and authentication—are a required part of the process. These professionals can now take steps to ensure that RADIUS is enforced in the device configurations. This whole exercise is simply about defining how your business works and how in theory it complies with whatever requirements you're facing, then communicating that information to the people who are tasked with ensuring that things really work that way.

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.

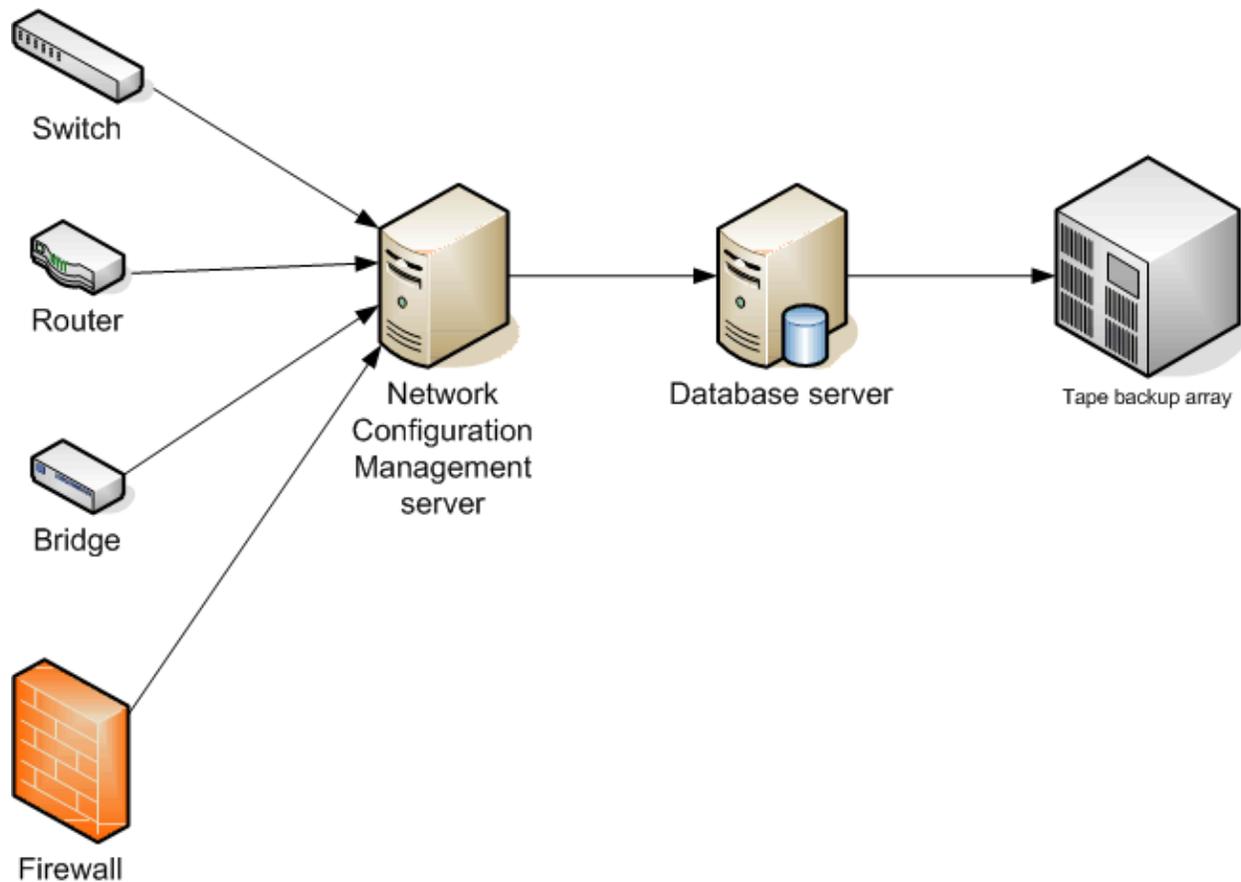


Figure 3.5: Using an external database for logging.

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.

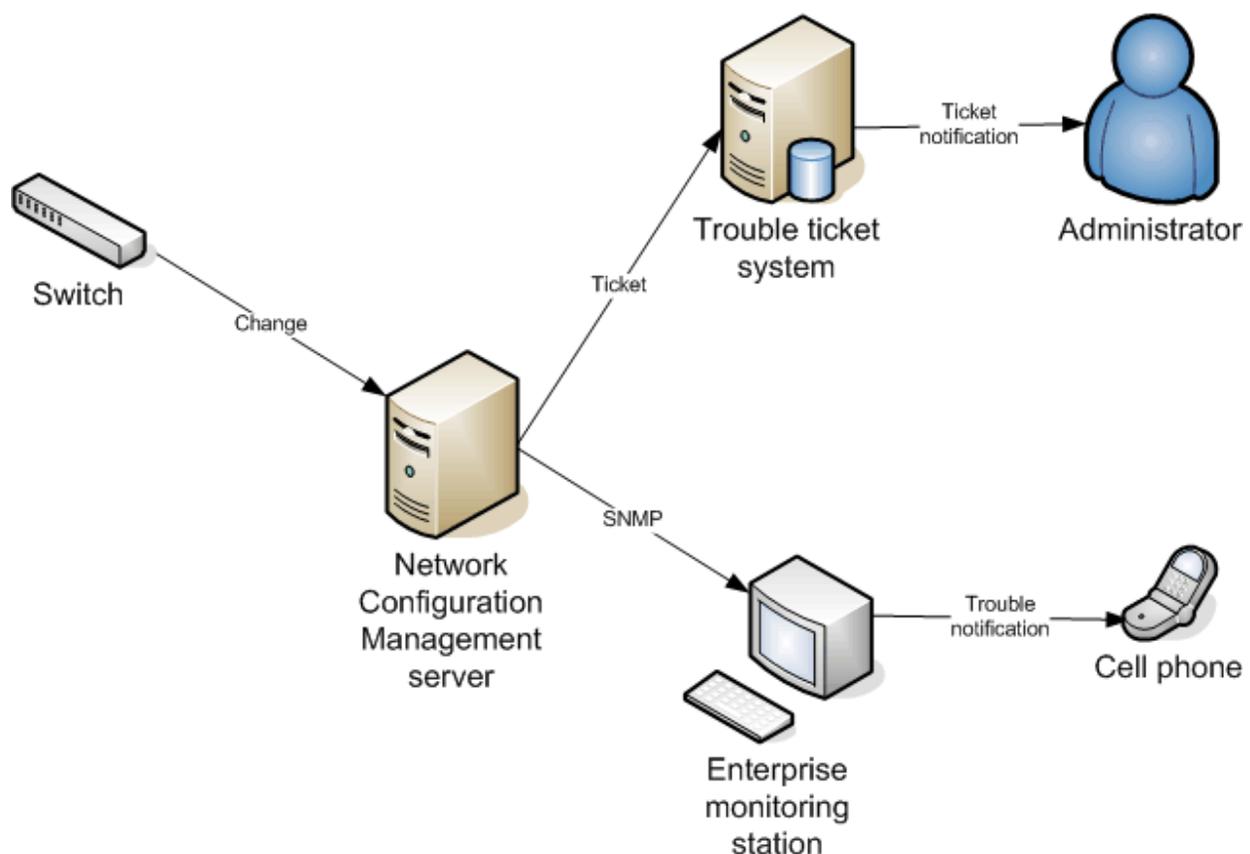


Figure 3.6: Integrating network configuration change notifications with your existing notification infrastructure.

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.

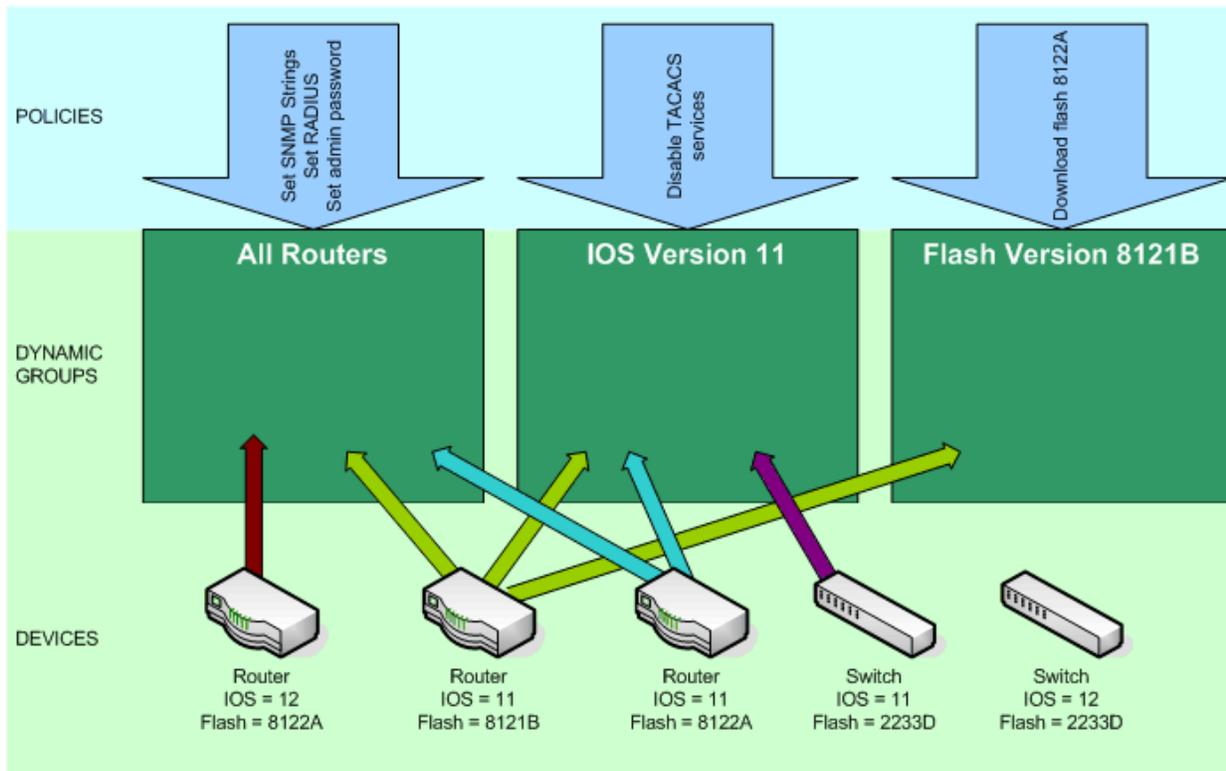


Figure 3.7: Dynamic groups can simplify complex policy application.

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.

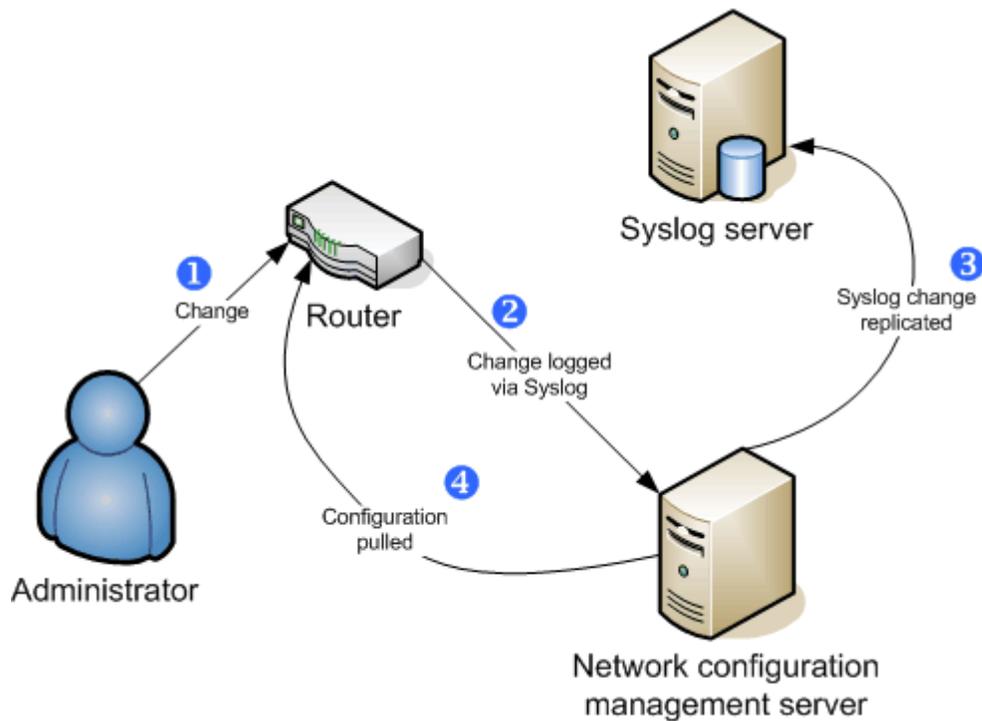


Figure 3.8: Using Syslog to receive change notifications and trigger a configuration analysis.

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.

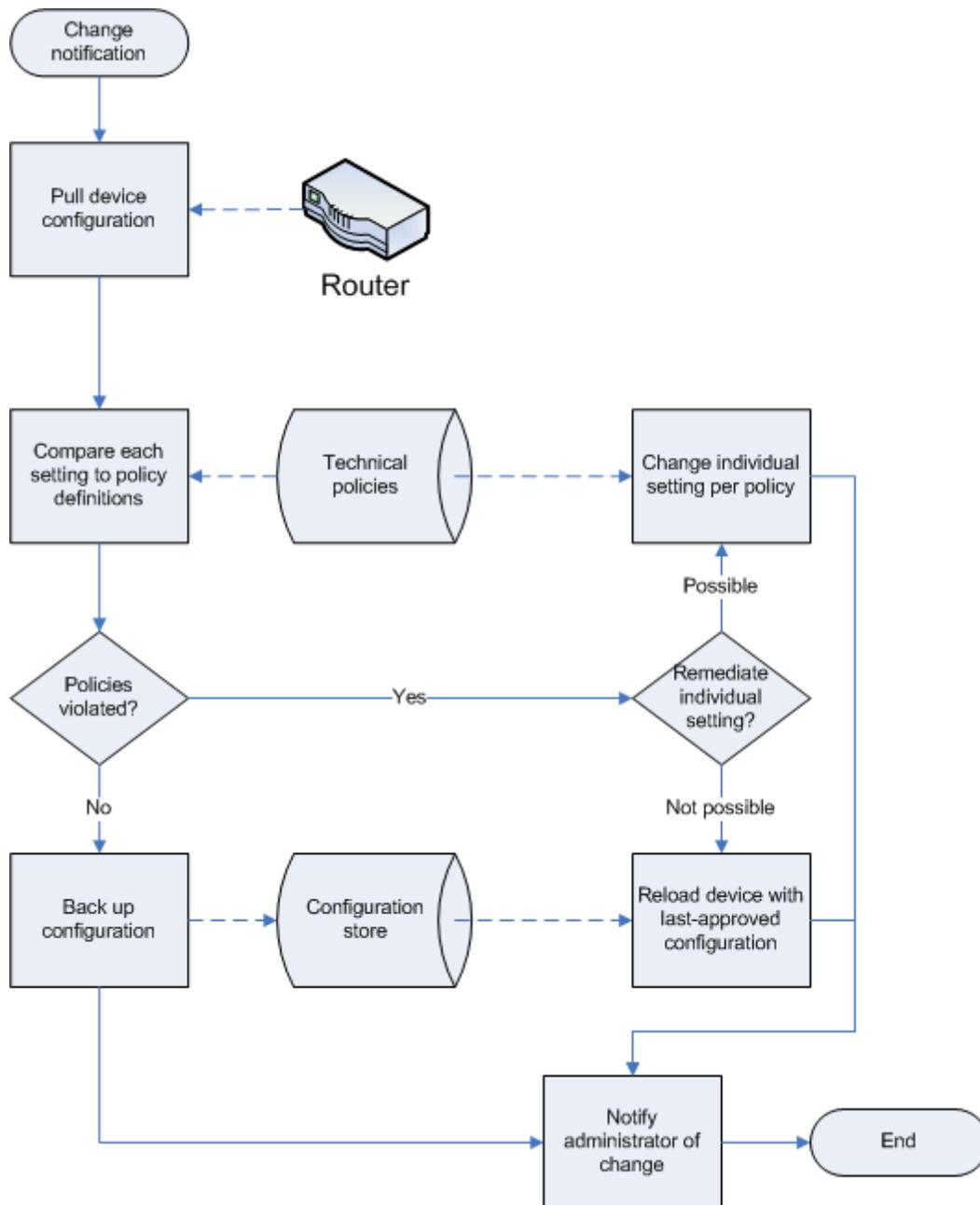


Figure 3.9: Basic process for automated enforcement.

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.