

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide[™] To



Automating Network Management and Compliance

sponsored by



i n v e n t

Don Jones

Chapter 2: Automating Network Compliance and Security	23
What Does the Network Have to Do With Compliance?	23
How Automation Affects Security and Compliance	26
Traditional Security and Compliance Loopholes	31
Overlooked Managed Elements	31
Point-in-Time Auditing Misses Changes.....	32
Direct Device Administration Causes Inconsistency.....	33
Inability to Tie Changes to Requests Reduces Accountability.....	33
Inability to Enforce a Configuration Management Process Affects Compliance.....	35
Inability to Effectively Report Makes Compliance Audits Difficult.....	35
Technologies and Tools that Close the Loopholes	35
Pass-Through Administration in a Management Solution.....	35
Automated Detection of Out-of-Process Changes.....	36
Automation of the Change Management Process.....	36
Role-Based Security in a Management Solution	36
Auditing in a Management Solution.....	37
Compliance Reporting	37
Automated Configuration Remediation.....	37
The Need for Auditing.....	37
End-State vs. Configuration Auditing.....	37
Network Management Through Templates and Policies.....	38
Automated Configuration of Devices	39
Building a Plan to Support Compliance and Security	39
Creating a Business Process That Supports Compliance and Security.....	41
Mapping Technologies to Your Business Process.....	41
Evaluating Solution Features that Support Compliance and Security	43
Evaluating Solutions' Ease of Adoption.....	43
Checklist: Tools and Technologies You Need.....	43
Summary	44

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.

[**Editor’s Note:** This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit <http://www.realtimepublishers.com/contentcentral/>.]

Chapter 2: Automating Network Compliance and Security

One of the biggest drivers behind the adoption of network automation technologies is the need for companies to improve their security and compliance postures. Security and compliance have become a major new requirement for most companies—any publicly traded company in the United States, for example, must comply with the provisions of the Sarbanes-Oxley Act—and the public and in-house attention devoted to compliance and security issues has become significant.

What Does the Network Have to Do With Compliance?

Most compliance legislation deals with considerations such as corporate accountability, customer privacy, and so forth; it’s not always immediately apparent how the network fits into the compliance picture. However, the network is the very basis of all information transmission in your organization—every file on a file server, every record in a database, and every Web page on a Web server is transmitted across your network. Network devices can include items such as firewalls and proxy servers, intrusion detection (or prevention) devices, and other elements that have an obvious impact on security. If a single router on your network is compromised, an attacker could conceivably route all traffic from that router to an unauthorized destination, exposing all your corporate data and creating a security—and potentially a compliance—breach. Almost every other data security measure your organization takes—securing file servers, locking down database access, securing ports on servers and client computers, and combating viruses and spam—is useless if the network becomes compromised. Because the network is used to transmit nearly all data within the organization, the network is the final point for compliance and security control.

How Legislation and Rules Affect the Network

Compliance begins with basic security. In general, legislation such as HIPAA, the Sarbanes-Oxley Act, and the Graham-Leach-Bliley Act, as well as rules like Visa’s Cardholder Information Security Program (CISP) merchant requirements, focus on the security and privacy of customer data. They also focus heavily on accountability, meaning you’re required to provide an audit trail of some kind so that all access to data, whether legitimate or not, is logged and can be reviewed at any time. At first glance, these broad requirements seem well-suited to a file server or database server, where data can be protected with access control lists (ACLs), data access can be audited, security logs can be aggregated and used to report on data access, and so forth. However, all of this access occurs over the network. Consider the functional diagram that Figure 2.1 shows.

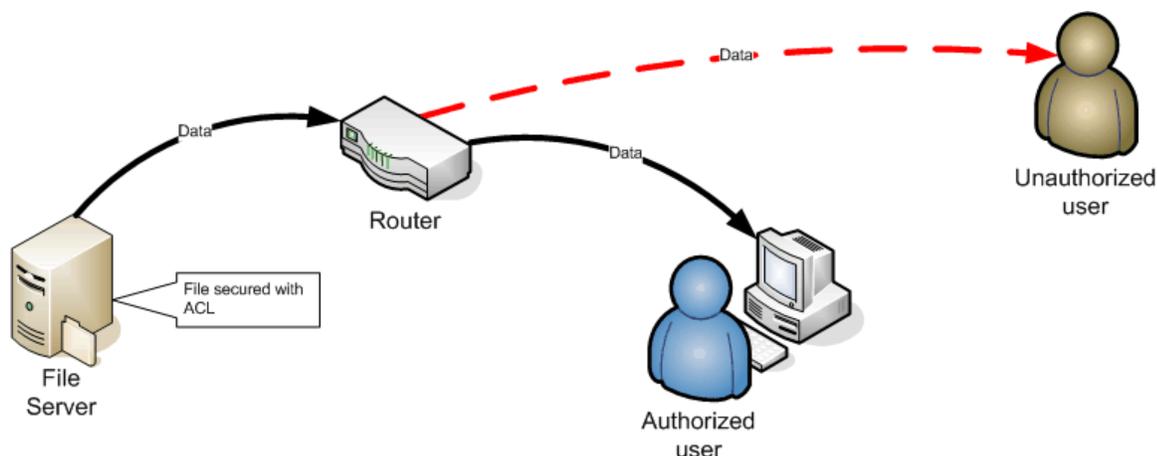


Figure 2.1: Functional diagram of data access.

In this figure, data on a file server is properly secured with an ACL. Auditing could also be configured so that data access can be tracked and reviewed. An authorized user accesses the data, which is transmitted to his or her computer across the network. However, in this example, the router's configuration has been modified by an unauthorized user, who is having the router send a copy of the information directly to him or her. The file server is unaware that this activity is occurring, so the unauthorized access isn't logged by the file server; the access, in fact, bypasses the server's security completely. In this way, the network is affected by compliance rules and legislation—the network offers a means of bypassing the more obvious security and auditing precautions you've put in place, which means the network can allow the activity that the rules and legislation are in place to stop.

Interestingly, compliance rules and legislation tend to say very little about how your environment should be configured, and instead focus on the end result. In other words, you won't find a legislative body passing laws requiring that file servers be configured to audit data access. Instead, the laws simply state (more or less) that *all* access to data must be logged. Thus, unauthorized access makes you non-compliant because you've failed to log a particular access to data. That means your network becomes a huge non-compliance liability, with all the associated financial and legal penalties. As outlined in the previous chapter, manually configured networks are highly susceptible to a number of conditions that make them more likely to be non-compliant.

How Network Operations Affect Compliance

Daily network operations—day-to-day configuration changes, for example—can have a significant impact on your network’s state of compliance. Remember, the compliance laws and rules don’t care about the actual state of your network’s configuration; they only care about the end result of that configuration. For example, suppose an administrator temporarily opens a firewall port to allow for a one-time activity—perhaps the administrator wants to play a game of networked Doom with a friend. The administrator closes the port when the game is over and puts everything back to the way it was. If nothing untoward happens during this period, you’re fine and you’re still compliant. However, if the administrator’s actions allow some private data to be disclosed without maintaining accountability, you’re non-compliant—you’ve broken the rules, and you may be subject to the consequences (which, of course, can extend far beyond mere fines or penalties; public disclosure of security breaches can cause significant market and financial harm).

In another example, suppose a new device is added to your network and configured according to a basic configuration template. However, the latest version of the device’s OS was not installed, perhaps leaving it vulnerable to attack—an attack which could compromise your compliance. The network technician logs the activity, but no mention is made of the installed OS version of the device in the report. This example highlights the fact that a manually configured and administered network is nearly impossible to properly maintain from a compliance and security point of view. Too many small changes or oversights can cause significant security harm, and those small changes and oversights are endemic to a manually configured environment.

How Networks Become Non-Compliant

In the end, nearly every action that happens or *doesn’t* happen to your network can affect your state of compliance. Making a small, improper change to a Simple Network Management Protocol (SNMP) ACL in a router, for example, can result in unauthorized, unaudited data access. Failing to apply a patch can result in the same outcome. A network in stasis—that is, one that doesn’t receive the latest patches and secure configuration changes—is sure to be a compliance problem eventually; conversely, a network in flux—one in which configuration changes are being made—is just as susceptible to becoming a security vulnerability. You can afford to neither leave the network nor make changes. *Manually*, that is: manual change of any kind is what ultimately leads to errors, inconsistencies, poor practices, and oversights—all of which lead to compliance and security problems.

Sometimes the path to non-compliance can be circuitous: Suppose an administrator deploys a new device and fails to change the configuration template’s SNMP community string settings. Because the template might be accessible to a broader range of people (after all, it’s just a text file with no special security significant in and of itself), that default SNMP community string might be well-known. That information can be used to reconfigure portions of the new device, thus compromising the device. Once compromised, the device can become a gateway for bleeding data off the network unnoticed or for introducing malicious software into the network. A seemingly innocent mistake—simply failing to change a text string consisting of a dozen characters or so—could result in an entire organization accidentally disclosing sensitive data with no accountability—a double hit on compliance.

The key, then, is to remove the manual configuration and administration from the loop. Your organization probably has, or is at least developing, business processes designed to ensure that changes don't create problems, and that the network is properly administered. Automating and enforcing that process is the way to a secure, compliant network.

How Automation Affects Security and Compliance

Automation is a concept that many IT managers and senior administrators hear constantly but don't always appreciate. They often think they know what automation is—scripts, written by administrators, to help make configuring multiple devices easier. That is certainly *one* form of automation, but frankly, it's the least-useful form. Although scripts are certainly better than manually typing configuration settings into devices, they still present many of the same problems as fully manual network management. If you must run the script manually, the process is still manual. True automation, however, goes far beyond mere scripts. And it's not just a marketing term invented by the companies who offer automation solutions; automation offers true business benefits that have a marked, positive impact on security and compliance.

How Automation Improves Daily Administration

Automation—that is, fully automated network configuration management solutions—can improve day-to-day network administration in a number of ways. Specific to security and compliance, automation can:

- Help ensure that no changes are made that violate specific compliance-sensitive portions of the network.
- Help ensure that changes are made consistently across devices, improving security.
- Help ensure that changes are made only when approved by a business process (which may include elements such as peer review), reducing errors that can compromise security or compliance.
- Help ensure that multiple changes to a device don't conflict by queuing changes and notifying change developers if the device's starting configuration is no longer the same as when a change was originally developed.
- Enable rapid deployment of changes to network devices.
- Allow illustration of ineffective or dangerous security changes before they are implemented.

For example, consider the diagram in Figure 2.2, which illustrates one way in which a configuration management solution might enforce security and compliance rules. As an example, suppose that the proposed change is modifying the SNMP configuration of a device, changing its read-write community string to Private. The solution pulls the device's current configuration, applies the change, then compares the new configuration with its database of configuration rules and policies. Such rules would often include a prohibition for the default community strings, such as Private, so the change would be rejected automatically and never applied to any device. The change to Private may have been accidental; it's possible the administrator creating the

change used a template file and just neglected to change that setting in the template. Regardless, the automation software caught the change before it was deployed, thus helping to maintain the security and compliance of the network.

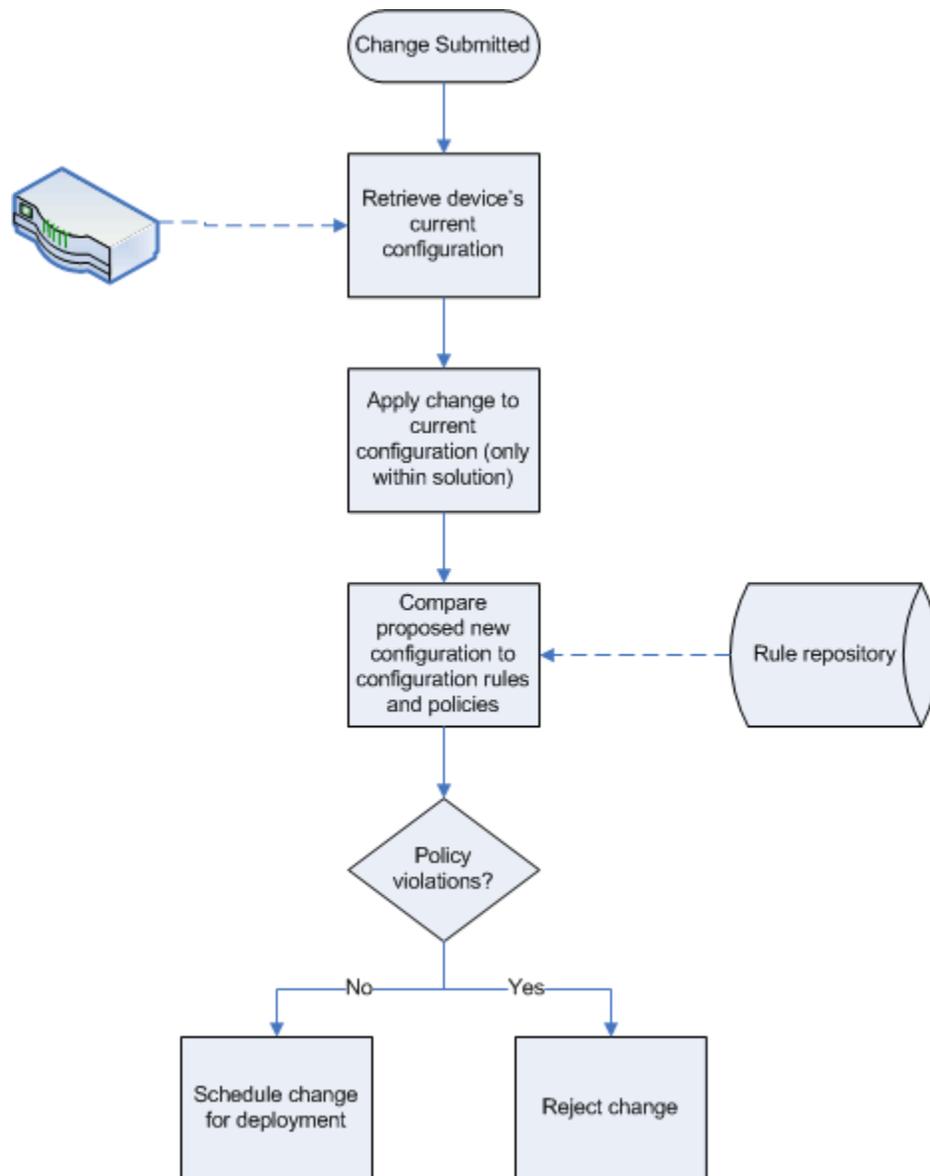


Figure 2.2: Automated change review process.

How Automation Adds Accountability to Network Operations

Accountability—being able to trace who made what change or who accessed which data—is a core concept of most compliance rules and legislation, particularly the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, and HIPAA. Network devices, however, have notoriously poor accountability built-in. Even when configured to use a logging technology such as TACACS+, RADIUS, or Syslog, network devices don't provide a high level of granularity. They might log

an event indicating that an administrator logged in, but don't expect your Syslog database to include details about what the administrator changed while logged into a device.

A much more granular level of accountability, however, can be achieved with a network configuration management solution:

- By performing all device administration through the solution, the solution can keep a detailed database of who made what changes, and who queried what data, from devices. Solutions typically implement their own security architecture, forcing users to identify themselves and tracking, in great detail, what each user does within the solution.
- Even traditional Telnet- or SSH-style administration activities can be performed through a configuration management solution, typically through a pass through or proxy mode. This ability allows the solution to log each keystroke from each administrative session, capturing the full scope of the session's activity and relating that activity to a particular user.

Figure 2.3 shows how this fine-grained auditing capability helps provide accountability that standalone network devices simply can't offer.

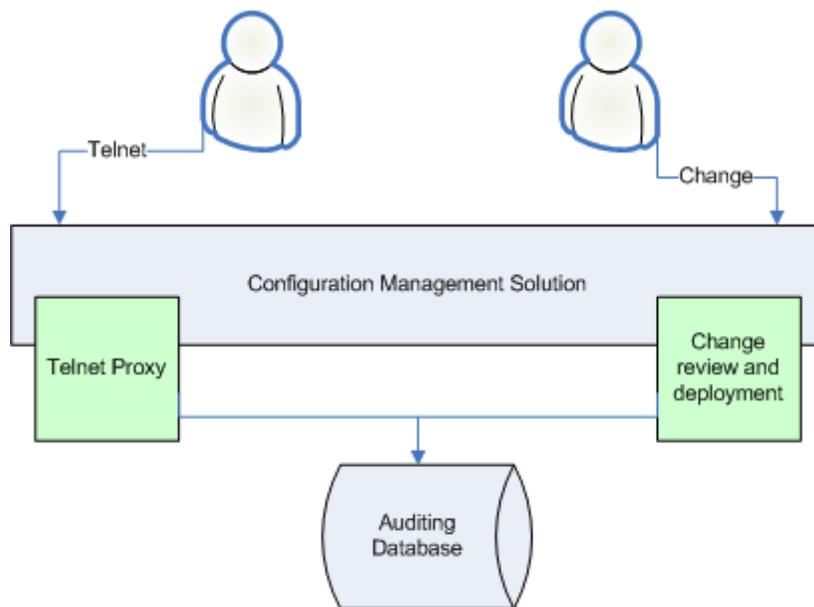


Figure 2.3: Auditing through a configuration management solution.

In fact, if your organization is subject to any accountability requirements—whether from internal governance rules or from legislation such as HIPAA, the Sarbanes-Oxley Act, and so forth—better accountability is the single best reason to implement a network configuration management solution. Without one, there is almost no way to provide fine-grained accountability and activity auditing for network devices.

Imagine being able to print a single auditing report that shows every single network device management action taken within a given timeframe. If you've ever been through a security or compliance audit, you know that this is one of the first things an auditor wants to see; if you can provide it, you've just made a potentially painful audit that much easier.

How Automation Ensures that the Network Remains Compliant

As mentioned earlier, a network configuration management solution can help a network remain secure and compliant by pre-approving day-to-day configuration changes using a preconfigured set of rules and policies to spot configurations that might violate compliance-related or security standards. Some network configuration management solutions go a step further by providing automated remediation capabilities (see Figure 2.4).

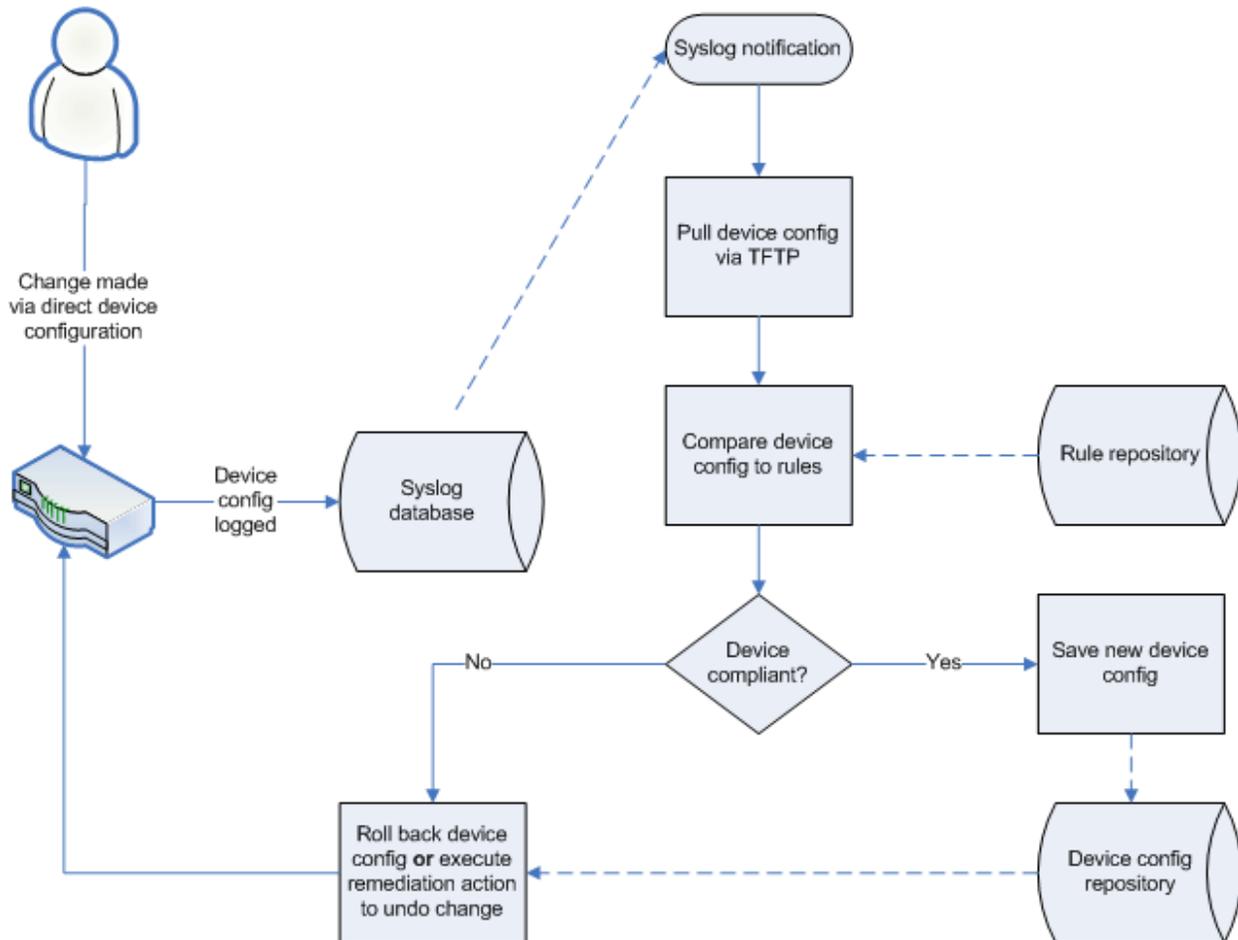


Figure 2.4: Automated remediation.

In this example, an administrator has made a configuration change to a device directly without using a network configuration management solution. That change—actually, the fact that the device was placed into configuration mode—triggers a Syslog (or TACACS+, or RADIUS, or SNMP trap) event. The network configuration management solution is configured to notice this event, and it triggers a configuration review process within the solution.

 Even without the event, the configuration management solution might be configured to pull device configurations on a periodic basis, at which time it would notice the change and perform the configuration review.

In the configuration review, the solution compares the current configuration with the solution's various rules and policies. If everything's okay, the configuration is saved to a repository as the "last known good" version of that device's configuration. If not, however, the solution can trigger an automated remediation response. Broadly, the solution might simply roll back the device's configuration, undoing all the changes and perhaps notifying someone of the action via email or SNMP alert. More specifically, the solution might have a remediation action associated with each of its configuration rules, allowing it to granularly undo just the change that violates a configuration rule or policy. Either way, the network's compliance is assured because non-compliant configurations are fixed automatically, within a few moments after the non-compliant configuration change was made.

Some network configuration management solutions come with (or offer as an add-on) preconfigured "packs" of configuration rules and policies specifically tailored to a given compliance environment: the Sarbanes-Oxley Act, HIPAA, the Gramm-Leach-Bliley Act, CISP, and so forth. These "packs" of rules can help get you up and running much more quickly, and can help you quickly determine which devices on your network are compliant.

Another way in which automation helps maintain compliance is through fast reporting. Because network configuration management solutions maintain a copy of each device's current (and past) configurations in a repository, they can examine those configurations quickly without having to physically connect to each device. This functionality makes compliance reporting much easier—you can simply run a report that lists which devices do and do not meet your configuration rules and policies. If those rules and policies define everything a compliance auditor would be looking for, your audit just became very, very easy—run the report. If it doesn't list any exceptions, you're done.

In fact, combined with automated remediation, compliance audits can often become a matter of looking at your configuration rules and policies to make sure they're comprehensive. If you can show that those rules cover everything, and that all your devices meet the rules—and thanks to automated remediation have *always* met those rules—the audit is over.

Traditional Security and Compliance Loopholes

Even with some forms of automation—such as scripted configuration changes—it's possible (and even easy) for security and compliance problems to arise. The reason is that network management technologies provide a number of loopholes through which improper configuration settings can creep in. The next several sections examine these loopholes and discuss how they can negatively affect the overall security and compliance posture of your organization. A discussion will follow with several sections about technologies and tools that can close these loopholes and keep your network more secure and completely compliant.

Overlooked Managed Elements

One of the biggest holes in most networks is managed elements—network devices—that the organization isn't aware they have. It sounds silly, but in an environment with hundreds of devices it's pretty easy to overlook one or two located in, perhaps, a remote office that doesn't have its own IT staff.

Overlooked devices represent the single biggest threat on any network simply because they're ignored—they don't get patched, they don't get the latest configuration changes, and they may not even get audited. They're completely off the radar, and as such can be compromised without you even being completely aware of where the breach came from. Once compromised, of course, you're no longer compliant or secure.

Most people don't believe ignored devices exist on their network. However, almost every organization that employs a network with more than a couple of hundred devices cannot provide a complete, written device inventory that matches what is really on the network. There is *always* one or two devices missing—perhaps a forgotten ISDN gateway that is used as backup connectivity on a remote network or an old router in a remote office that is quietly humming along, doing its job, and not attracting any attention.

Other times, the overlooked devices are ones that never should have been there in the first place. A field engineer, for example, hooking up a router for testing purposes without telling anyone—then leaving it hooked up forever. Or rogue wireless access points connected in branch offices or in departments to provide wireless coverage that the company isn't officially providing. They are often connected by well-meaning employees who just want to connect their laptops. They do not know or understand WEP keys, hiding SSIDs, or even changing the default password to configure the device. They provide access to anyone with an 802.11 device within range of the device—whether they work for your company or not. *Any* of these can quickly become a security problem; if a compliance auditor runs across a device that you don't know about, your audit will not go well no matter how well the device is configured.

Unless you're using some form of automation—and many companies are, now, for device discovery if nothing else—then you probably have forgotten devices floating around on your network.

Point-in-Time Auditing Misses Changes

Compliance is not about auditing. Compliance is about meeting the letter of the law—ensuring that data isn't disclosed to unauthorized parties, ensuring that full accountability exists, and so forth. Auditing is just a spot-check to make sure you're doing it, but be very clear in your mind that, as a means of actually enforcing compliance—that is, ensuring that you're continuously obeying whatever laws or policies apply to you—auditing is nearly useless.

For example, a major East-coast telecommunications firm had a security policy regarding the frequency with which user passwords had to be changed—a common policy. However, the environment contained a number of disconnected systems, each with their own passwords, and users weren't exactly technical experts. Thus, the password change requirements were turned off. When an audit came—and the firm always knew at least a few hours in advance—the change requirement was turned on again. When the auditor left, so did the change requirement. In effect, the firm was compliant with its policies for however long the auditor was in the building, and passed every audit. Usefulness of audit? Zero.

The problem is that auditing represents a very small point in time, and networks change too much and too quickly for that point in time to have a practical purpose. Instead, organizations need to practice *continuous enforcement*. For example, if the telecommunications environment had included a configuration management solution, the auditor would have been able to look at a simple report and see that administrators had been tweaking the password change requirement setting, and that the firm hadn't been compliant for more than a few hours each year. In fact, the configuration management solution could have easily overridden the password requirement changes, reconfiguring the password change requirements every time they were turned off. Such a system would have enforced the company's policies continuously. Of course, back then such technologies weren't available—but they are now.

Direct Device Administration Causes Inconsistency

Manual administration—meaning administration through direct interaction with network devices—is the primary cause of inconsistency and inconsistency is a major factor in security and compliance problems. Direct device administration is simply too prone to manual error. This sometimes applies even to proxied device administration, where administrators actually use a network configuration management solution to Telnet or SSH into a device to administer it. Although the solution can log keystrokes for auditing purposes, many solutions don't analyze the session's contents to determine whether a security or compliance rule is being violated. Some solutions do—they're able to review changes as they're entered into the Telnet session, determine whether the changes violate any configuration rules, and prevent the change from actually being sent to the device (or at least warn the administrator that there is a conflict). However, no solution can completely prevent direct device administration from occasionally causing problems and configuration inconsistencies.

Inability to Tie Changes to Requests Reduces Accountability

At the core of any truly secure and compliant network is a comprehensive business process, such as the one shown in Figure 2.5.

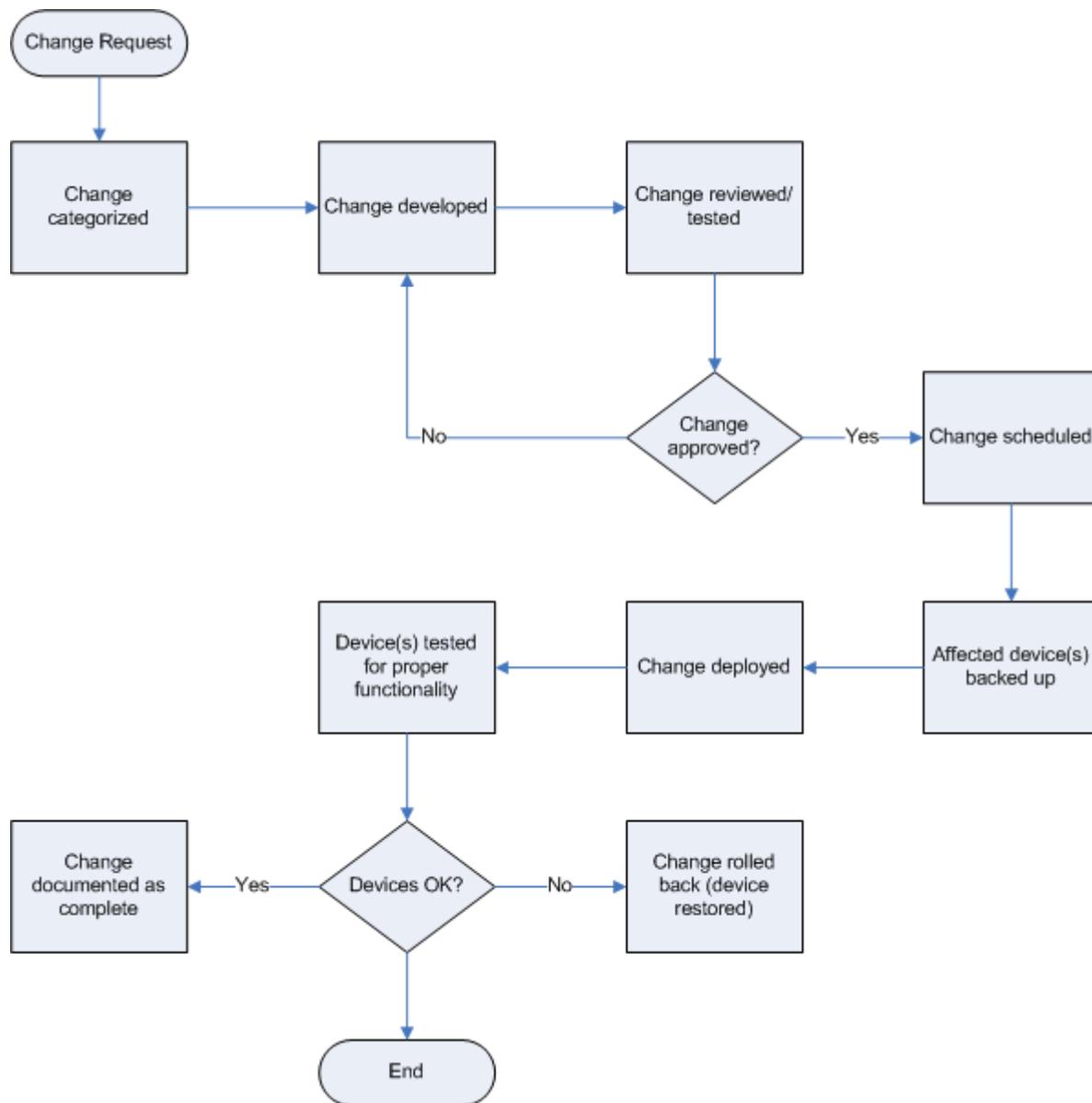


Figure 2.5: Sample configuration management business process.

Unfortunately, without some sort of automated system in place, it's too easy for changes to occur outside this process. Out-of-process changes are not inherently bad, but from a security and compliance standpoint, you want to always be able to relate any change to the original, in-process change request. That is, no change should exist without a corresponding change request, thus helping to ensure that changes have all made it through your change management process.

Inability to Enforce a Configuration Management Process Affects Compliance

Ultimately, it's *enforcement* that is the loophole. Without automation, it's too easy to bypass whatever safeguards your organization may have put in place to prevent insecure or non-compliant configurations from being put into production.

You can't effectively test or audit the end-state of a secure, compliant network; instead, you simply have to come up with a configuration that does the job and ensure that the configuration stays in place. If there is no process managing change, or if there is a process that can be bypassed, then changes that are insecure or non-compliant can occur to configurations. Simply having a process isn't sufficient; it must be enforced, and in a manually configured network that's practically impossible to do.

Inability to Effectively Report Makes Compliance Audits Difficult

Compliance audits are the low point of most administrators' and managers' work lives—auditors run around, asking for difficult-to-provide information, asking difficult-to-answer questions, and generally making everyone's lives difficult-to-live. And the auditors aren't any happier about it; they're simply there trying to do a job and ensure that the network is (and has been, and likely will be) secure and compliant, yet they have precious little information to work with. This situation is a huge loophole in the compliance (and security) world, because the audit is the last point at which compliance and security problems can be caught. Without information to work with, audits are completely ineffective. In fact, most organizations struggling with audits aren't struggling with their actual device configurations as much as they are struggling with simply trying to provide their auditors with the right information.

Technologies and Tools that Close the Loopholes

So how can you close the loops in traditional device management without removing critical functionality and capabilities that your organization and its staff require? Automated configuration management solutions can provide most of the answers.

Pass-Through Administration in a Management Solution

Pass-through administration—sometimes called *proxy* administration depending on how it's implemented—allows administrators to continue using Telnet, SSH, or other command-line administration techniques. One of the biggest fears presented by a new automated configuration management solution is that administrators will be crippled and unable to access devices in the ways they need to in order to properly maintain the environment. Such shouldn't be the case, of course; a well-designed solution can provide capabilities such as Telnet. Because the Telnet (or SSH, or whatever) traffic is passing *through* the configuration management solution, the traffic is also auditable and can be secured using the solution's own more granular, role-based security.

Automated Detection of Out-of-Process Changes

Regardless of which type of solution you have in place, however, out-of-process changes are practically a certainty in any organization. You can try to reduce these as much as possible (and you should), but they're still likely to occur, meaning they still represent a major loophole to security and compliance in your environment. However, a good configuration management solution can still deal with out-of-process changes, in two ways:

- By reading SNMP traps, TACACS+ logs, and Syslog logs, the solution can “know” when a device may have been changed, and use that knowledge to examine the device’s configuration.
- On a periodic basis, the solution can simply re-read all devices’ configurations to look for any changes it might have missed.

These out-of-process changes can then be examined for consistency and compliance with your configuration rules, and alerts can be generated to let someone know that devices have been reconfigured outside of the configuration management solution.

Automation of the Change Management Process

A good configuration management solution can also automate and enforce your business processes. For example, some solutions can integrate to some degree with Help desk management solutions and with enterprise management frameworks, allowing them to initiate changes based on incoming Help desk tickets. Some solutions, for example, might not allow a device configuration change to be initiated until a Help desk ticket can be linked to the change, thus ensuring that any formal review process you may have in place is followed. The solution can also enforce peer reviews by not allowing changes to be deployed until an authorized user reviews and approves them. Maintenance windows can also be enforced by preventing changes from being deployed outside the window without special approval. One of the major loopholes in security and compliance is the ability to enforce your business processes; configuration management solutions can provide that enforcement.

Role-Based Security in a Management Solution

Network devices typically don’t have very granular security; it’s pretty much “read” or “read/write” to the devices’ configurations. A configuration management solution can provide much more granular, role-based security, allowing the right people to read and write the configurations of the appropriate devices. In fact, some solutions provide such granular security that you can designate a particular role as being able to read, read and write, or have no access to *individual items within a device’s configuration*. A particular role might, for example, be able to read and write the SNMP community string from just a specific subset of your network’s devices. Regardless of whether you need that level of security, having the capability provides you with a great deal of flexibility to ensure your network remains properly configured and that configuration data is available only to the people who absolutely need it.

Auditing in a Management Solution

Management solutions typically provide detailed reports that can be a real blessing when the time for an audit rolls around. Reports may simply list all unauthorized changes (an empty list would make the auditors happy), all changes made in a certain date range (for comparison to the change requests you maintain), and so forth.

Because most management solutions provide detailed auditing records, everything an auditor might need to know—including current device configurations—is immediately available. Auditors can be given permission—through the solution’s role-based security—to read (but not change) any data they might require access to, and they’ll never have to log into a single network device because all the information is maintained within the solution’s own database.

Compliance Reporting

Solutions that come with compliance-specific reports (for example, Sarbanes-Oxley-specific reports are becoming common in more high-end solutions) can make compliance audits even easier. By simply running the appropriate report, you’ll be able to provide a compliance auditor with almost everything they need to know to complete their audit. They won’t have to dig for information, you won’t have to spend days assembling the reports, and everyone’s lives will be much easier.

Automated Configuration Remediation

Finally, the ability for a network configuration management solution to quickly and automatically reconfigure devices to match your configuration rules and policies is invaluable. Everything up to this point has been about ensuring the right configuration gets to devices, but automated remediation is the last line of defense when improper configurations make it out to devices anyway. Rather than simply alerting you to a problem—which is useful but still allows the problem to exist for however long it takes *you* to deal with it—automated remediation helps keep you secure and compliant *at all times* by ensuring sensitive configuration settings are never changes for more than a few minutes without being automatically reset to your centrally configured, top-level rules.

The Need for Auditing

Auditing *is* a necessary function. However, it’s important to realize what auditing can and cannot do, and what it can and cannot tell you so that you’re auditing the right thing. IT in general, and networks in particular, don’t lend themselves well to configuration spot-checks. That doesn’t mean auditing is entirely useless, but it does mean that the auditing performed by most organizations is effectively useless. The next few sections outline effective auditing.

End-State vs. Configuration Auditing

One important concept in auditing is the idea of auditing the *end-state*. For example, if Ford claims that their cars can protect a passenger in a 20mph frontal collision, auditors don’t sit down and examine the car’s engineering drawings; instead, they crash the car into a steel wall using

test dummies to see how the dummies fare. This is the *end-state*—testing the final outcome of the claim.

However, this process is pretty much impossible in networking. If you claim, for example, that no unauthorized individual can access data, you can't *prove* it directly. For one thing, you'd have to have every man, woman, and child on Earth give it a try. For another thing, there are factors involved that are completely outside of your control. An operating system (OS) bug, for example, could result in your claim being false, despite your best efforts. Thus, in the world of IT and networking, you instead do the equivalent of looking at the engineering drawings: You examine configurations to determine whether they're likely to meet your claims. You use documented best practices and other materials to develop what you think are secure configurations, and you check to make sure they remain in place.

Thus, the first thing to understand about network auditing is that you can't audit the end-state. Instead, you can audit only the configuration. Because you're relying on the configuration, you need to ensure that it's been in place *continuously* (a concept covered earlier in this chapter). You must also recognize that individually auditing the configurations on an organization's hundreds of network devices is exceedingly time-consuming; most auditors content themselves with a spot-check of a few devices, which is pointless because just one misconfigured device is all you need to make an organization insecure and noncompliant. As you must acknowledge your inability to test the end-state and to be comfortable just auditing the configuration, there has to be a more effective way than per-device auditing.

Network Management Through Templates and Policies

Managing through templates and policies, rather than managing actual device configurations, makes much more sense when you have a need to maintain security and compliance on your network. Think about it this way: What if you could create a set of configuration rules and policies, then have a network configuration management solution automatically enforce those rules and policies? Any device on your network that didn't match up with the rules and policies would be fixed immediately. If you needed to change one of your rules, you'd simply *change the rule*. All your devices wouldn't match the new rule, so your configuration management solution would *automatically reconfigure them*. True, it takes a bit of experience and trust to come to the point where you can do that with a configuration management solution, but this style of management is incredibly flexible and really helps to implement the top-down type of management espoused by IBM in its OnDemand framework and by Hewlett-Packard in its Adaptive Enterprise framework (and by Microsoft in its Dynamic Systems Initiative, for that matter). Stop managing devices; instead, manage policies and have a solution that makes your devices comply with your policies.

In such a situation, think of how simple auditing would become—an auditor checks your policies to make sure they're right and checks to make sure your solution is enforcing those policies. Audit done. This top-down type of administration is possible without an automated network configuration management solution, of course, but it isn't efficient, and because it requires devices to be manually reconfigured to match policies, you're really still just managing individual devices.

Automated Configuration of Devices

Automated configuration is, as in so many other areas, the key to making auditing easier. Remember that network devices were, for the most part, never intended to be audited. Sure, they have some logging capability, and thanks to technologies such as Syslog, RADIUS, and TACACS+, it is possible to do a halfway decent job of tracking changes. However, network devices just weren't built to be auditable devices. Automated configuration brings the actual configuration activity out of the device and into a much more auditable and accountable environment in which very granular auditing records can be maintained. Finished configurations are pushed out to devices that still aren't very auditable, but provided the configuration solution is the *only* means through which to modify device configurations, it doesn't matter; all the auditing information you'll need is contained within the solution itself.

Building a Plan to Support Compliance and Security

An automated configuration management solution should exist primarily to support a business process, such as one that follows the Information Technology Infrastructure Library (ITIL) framework for change and configuration management. Creating an appropriate business process, then, should become your first order of business. For an example that provides a quick overview and a sample business process, consider the process in Figure 2.6, which is an expansion of Figure 2.5.

This process doesn't refer specifically to technologies (my notes, in yellow callouts, suggest technologies, but the main process steps, in blue, don't). The reason is that this is a *business* process, and it could easily apply to almost any type of configuration management activity, not just network devices. The process has a few characteristic steps:

- Changes are received and logged
- Changes are reviewed and categorized, often by a small group representing both technical and management concerns
- Changes are developed by technical resources, such as administrators
- Changes are reviewed
- Changes are scheduled for deployment inside maintenance windows
- Devices are backed up prior to being changed
- Devices are tested after the change is deployed
- Feedback into the Help desk system—closing tickets, for example—closes the loop and ensures the original request is fulfilled by the change

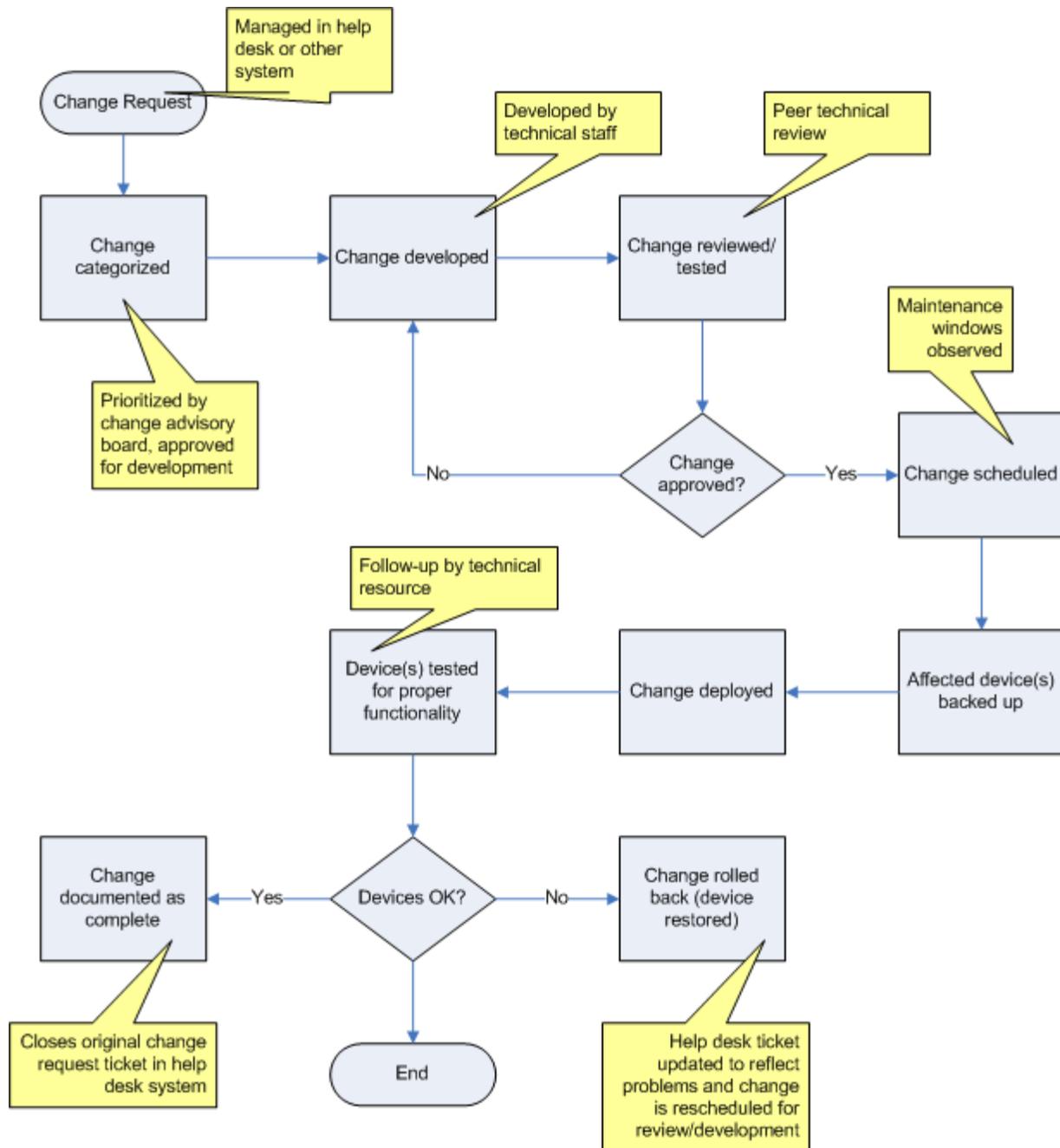


Figure 2.6: Sample configuration management business process.

Creating a Business Process That Supports Compliance and Security

Any business process can be tweaked to support compliance and security. In the example process, most of the requirements a secure and compliant organization might have are already represented:

- Changes are initiated by a logged, auditable request
- A review process ensures that changes are done correctly and that they don't violate any security or compliance rules
- Changes are tracked through to completion by being tied to a "request," such as a Help desk ticket.

The trick, of course, is in *enforcing* this process, as a process' mere existence doesn't ensure that it'll be followed.

Mapping Technologies to Your Business Process

Bringing in technology to support the business process is the next step. For example, Figure 2.7 shows the same business process, with ideas about how technology and tools can fit in to handle or support various steps of the process; the items in orange can usually be provided by a high-end configuration management solution.

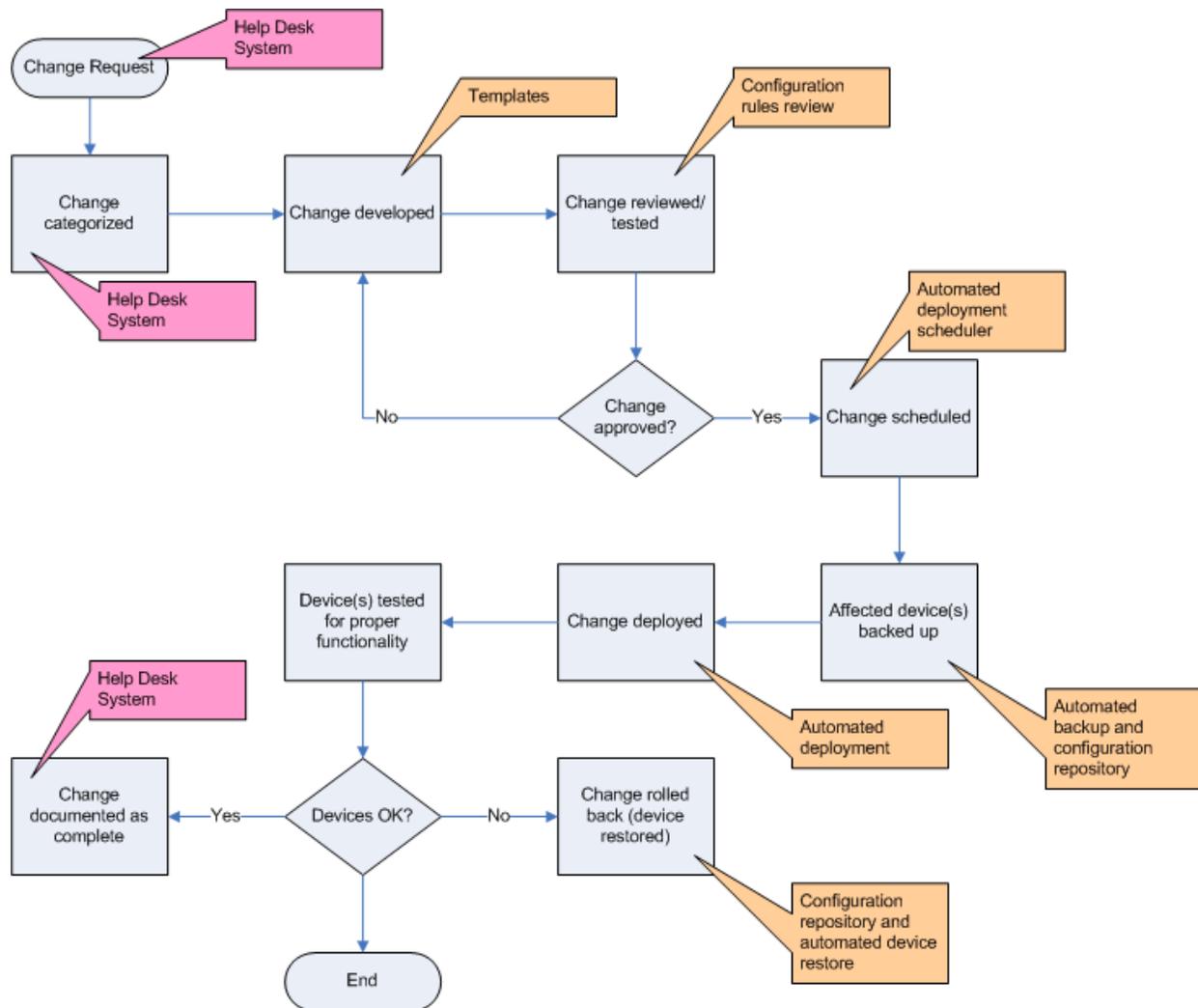


Figure 2.7: Adding supporting technologies.

Understanding that *this* is your business process and *these* are your technological needs will allow you to begin evaluating solutions to find ones that meet your technological needs. This process is different from simply looking at solutions to see what they all can do; that usually winds up in the acquisition of something that *doesn't* support your business processes, meaning your business will have to change to accommodate the technology—and that's rarely a good idea.

Evaluating Solution Features that Support Compliance and Security

Once you've identified your business and technological requirements, start looking at configuration management solutions. Ask detailed questions about *how* each solution supports each of your needs; vendors all have different approaches, and you want to find the one that seems to do the best job for your organization. Be cognizant of implementations that might require more training for your staff; this requirement is not necessarily a bad thing, but you want to be aware of that requirement up front. Construct an evaluation form that allows you to document how a solution addresses each of your needs, and ask others in your environment to review the form and generate follow-up questions. Create a scoring system that allows you to weight each solution's desirability based on how well it addresses your specific needs. As you learn more about the products you're evaluating, fine-tune your technological requirements: You may, for example, learn that some products interface with an enterprise management framework that you already have, and might choose to make that a requirement of whatever solution you eventually choose.

Evaluating Solutions' Ease of Adoption

The last thing to check out is how easily a solution can be adopted and deployed. Ask vendors for case studies and customer references; ask detailed questions about how long it takes to deploy the solution, get your configuration policies into it, and so forth. How long will it be, and how much will it cost, until the solution is fully in place and supporting your business requirements? Will your staff need special training? Is the deployment phase something the vendor (or a partner) can assist with?

Checklist: Tools and Technologies You Need

The following list provides a basic checklist of the things you'll need in your environment in order to make automation a reality:

- TACACS+, RADIUS, or Syslog, with all network devices logging to whichever one you select
- SNMP
- Automated backup of device configurations into a configuration repository
- Automated deployment of approved configuration changes
- Enforced workflow for change development, approval, and scheduling
- Ability to specify configuration rules or policies, which can be reviewed by the solution so that you can see which devices match and which don't
- Ability to *enforce* configuration rules and policies, perhaps by tying a corrective configuration action to each rule so that devices in violation of the rule can be automatically remediated
- Pass-through or proxying for Telnet or SSH so that administrators can continue using existing practices to manage devices

These are, of course, just the basics—you'll likely have additional requirements, but this list should help get you started.

Summary

Although the network might not seem to have an obvious role in compliance and overall organizational security, it is in fact the one point at which everything comes together; the bottleneck, if you will, for security and compliance. The reason is that networks transmit most organizational data, and yet networks are inherently more difficult to secure and protect than the repositories—such as file servers and databases—where data normally resides.

Creating a secure, compliant network virtually *requires* automated network management tools because a manually administered network is nearly impossible to make compliant and keep that way. Even with a compliant, secure business process for making network configuration changes, too many loopholes exist that can take the network into an insecure, noncompliant state. Automation can close these loopholes by automatically detecting devices, automatically detecting configuration changes, enforcing a configuration management workflow, and ensuring that your known-compliant configurations are in fact active throughout the network. Network automation solutions can ensure that your business processes are enforced and effective, and can provide the on-demand reporting and configuration management controls you need to maintain a fully secure, fully compliant network at all times.

Content Central

[Content Central](#) is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, [Content Central](#) offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: <http://www.realtimepublishers.com/contentcentral/>.