

[**Editor's Note:** The following excerpt is from the free eBook *The Shortcut Guide to Network Compliance and Security* (Realtimepublishers.com), written by Don Jones and available at <http://www.alterpoint.com/support/complianceEBook/registration.jsp>.]

Chapter 4: Network Compliance Best Practices and Methodologies

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

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

The ITIL Framework

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

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

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

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

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

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

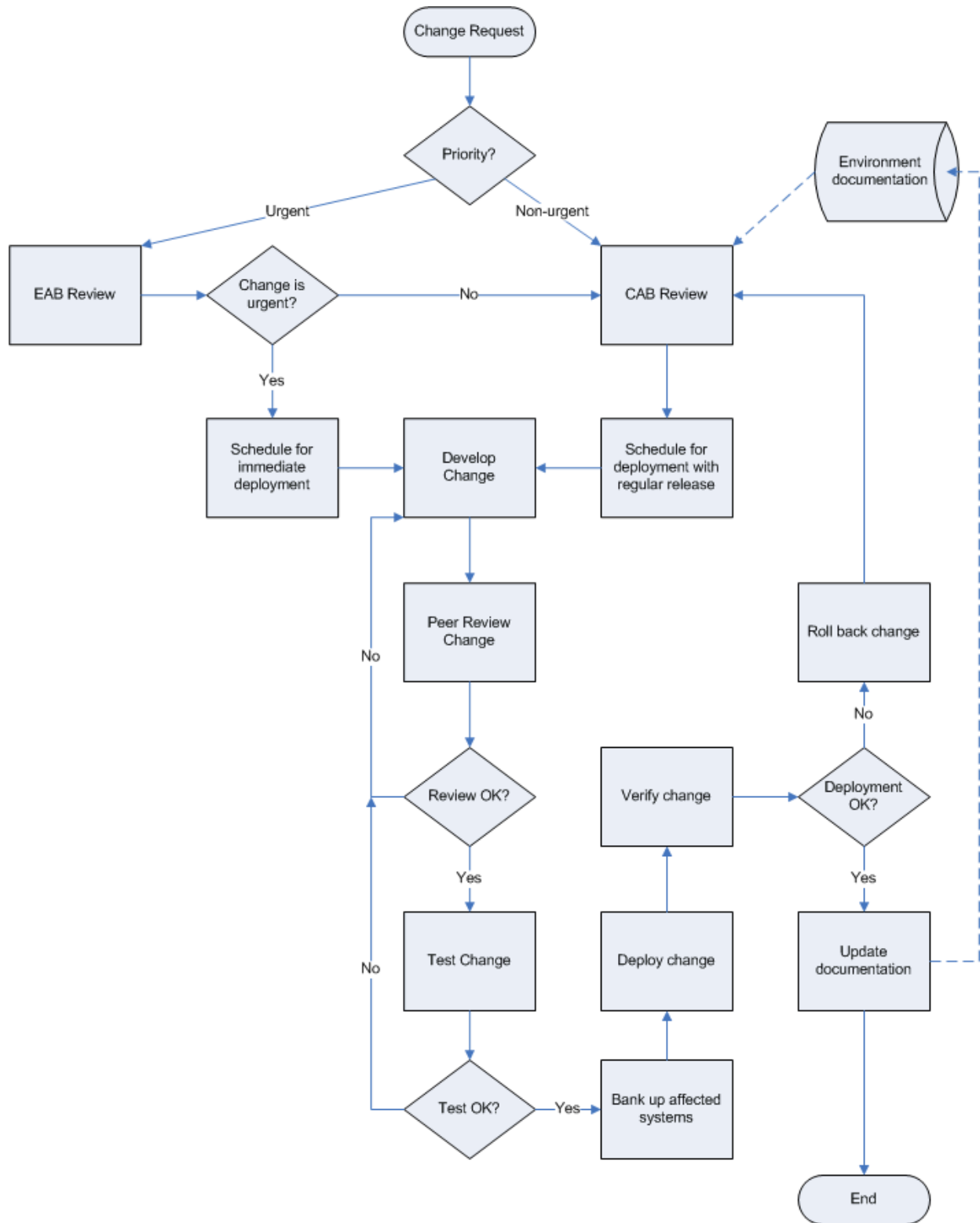


Figure 4.1: Simplified ITIL-inspired change management process.

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

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

Singles or Batches: Risks of Making Changes

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

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

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

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

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

Network Compliance Management

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

Assemble Your Business Policies

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

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

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

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

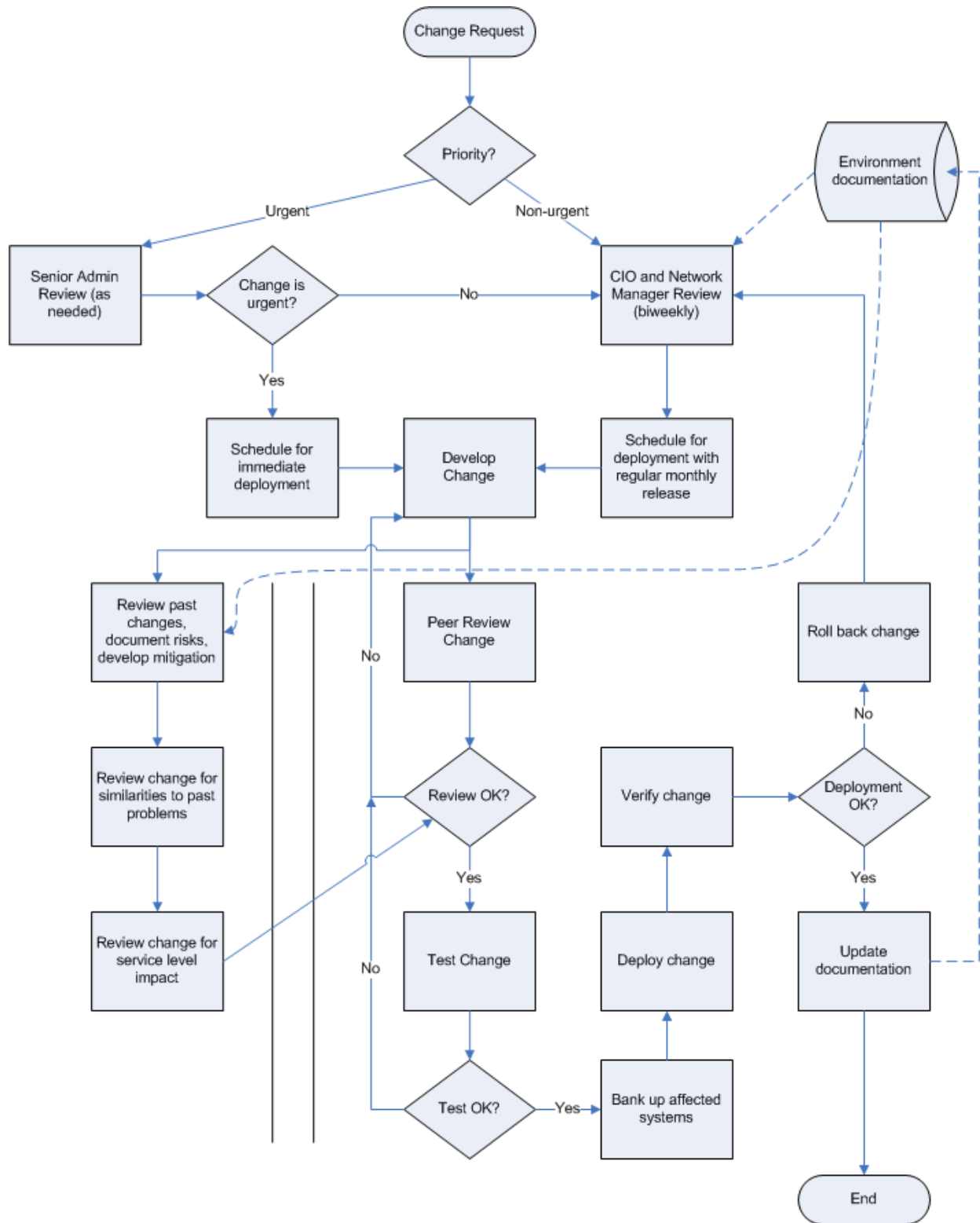


Figure 4.2: Adding business-level concerns to a process flowchart.

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

Integrate Legal Requirements

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

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

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

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

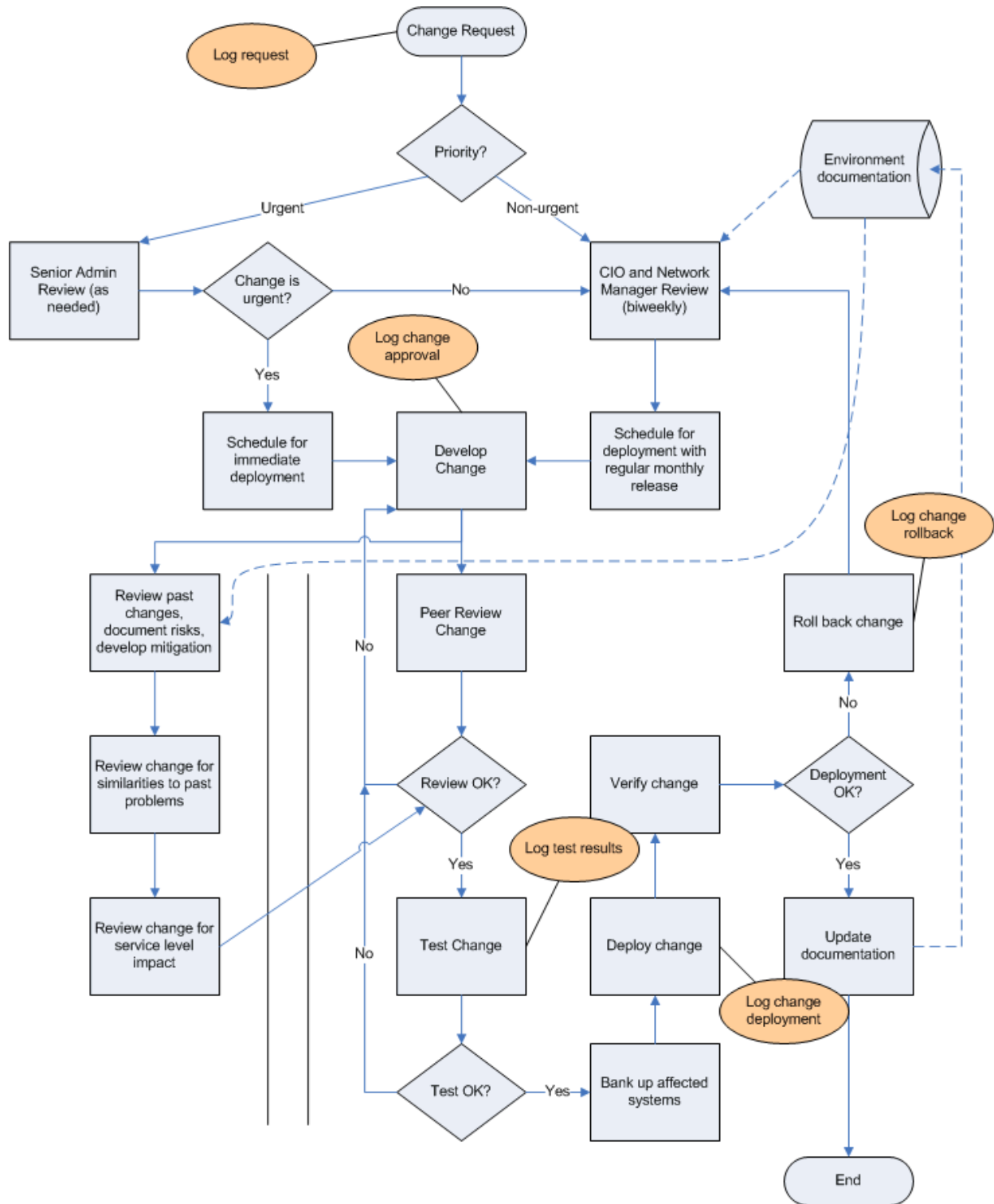


Figure 4.3: Adding legal requirements to your management processes.

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

Layer in Security

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

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

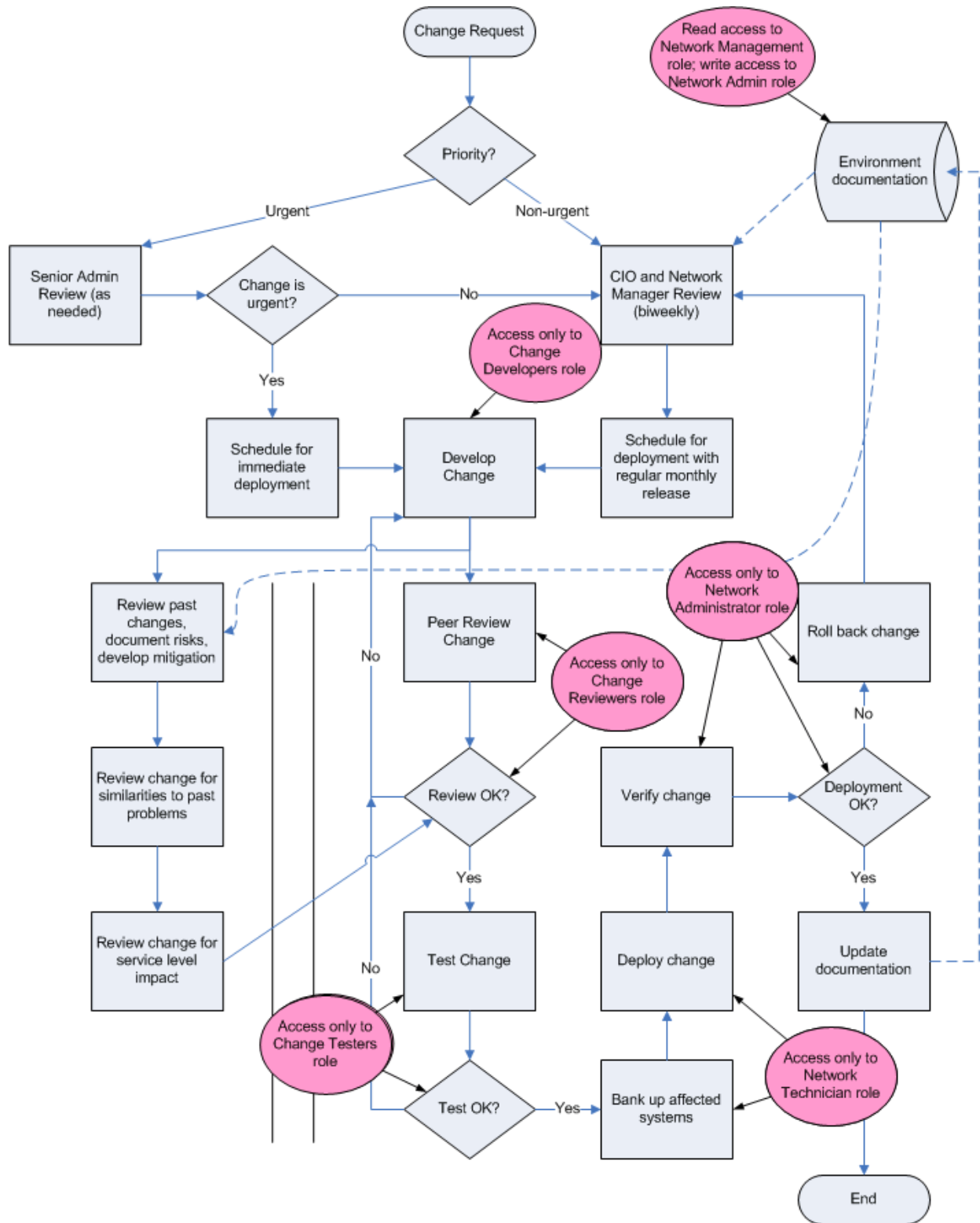


Figure 4.4: Adding security-specific concerns to a business process.

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

Create Your Final Business Policies

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

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

Applying Management Policies

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

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

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

Inventorying Your Network

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

Inventorying Your Needs

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

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

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

The Right Tool for the Right Job

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

Evaluating Management Tools

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

Feature by Feature Comparison

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

72

103

Figure 4.5: Evaluating tools that meet your needs.

Matching Your Tools to Your Processes

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

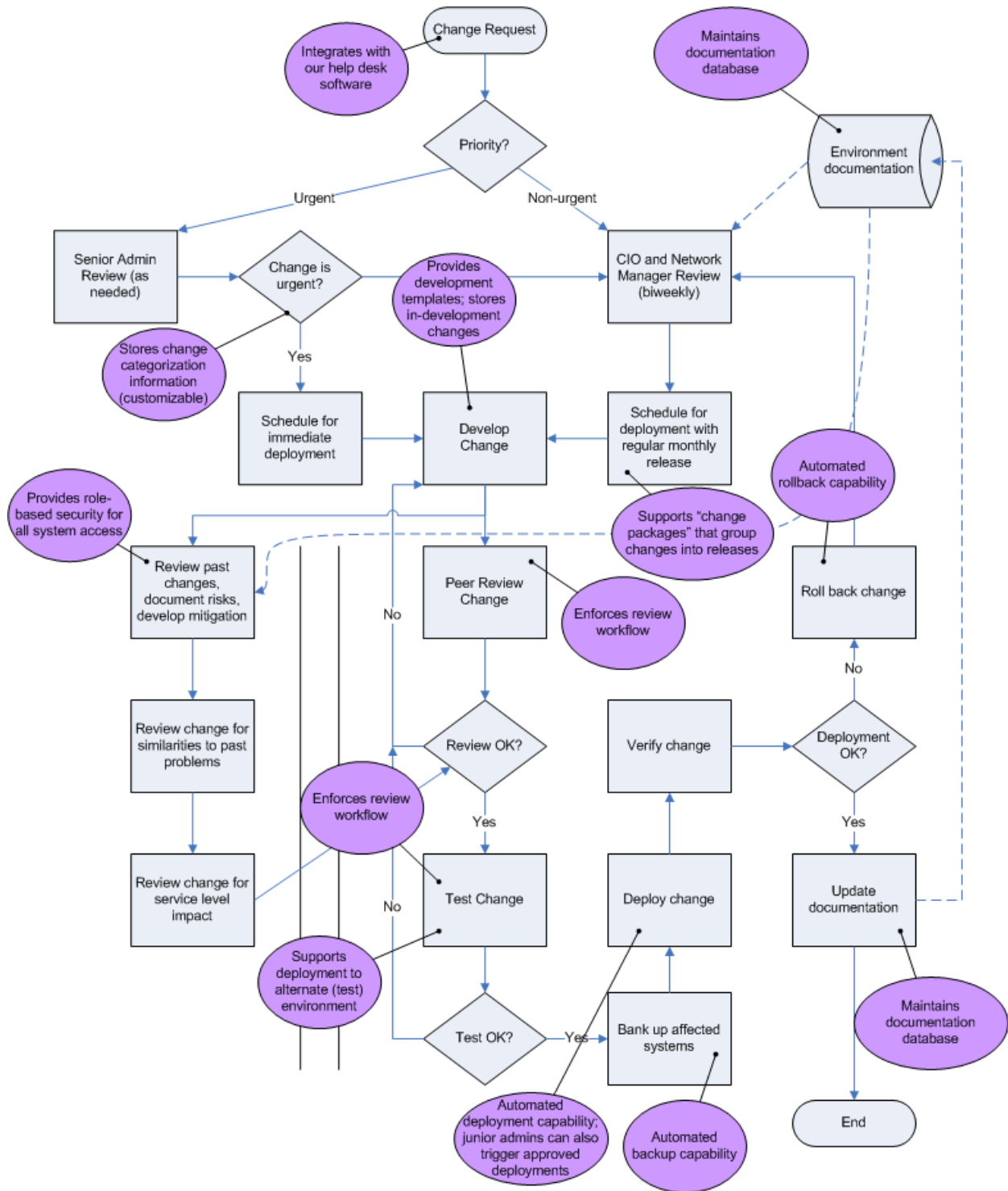


Figure 4.6: Mapping a configuration management tool to my processes.

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

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

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

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

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

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

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

Summary

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

[**Editor’s Note:** The following excerpt is from the free eBook *The Shortcut Guide to Network Compliance and Security* (Realtimepublishers.com), written by Don Jones and available at <http://www.alterpoint.com/support/complianceEBook/registration.jsp>.]