Realtime
publishers

"Leading the Conversation"

The Shortcut Guide™ *To*

Automating Network Management and Compliance

sponsored by

hp invent

Don Jones

Copyright Statement

Chapter 4: Building the Plan for Automating Network Operations

Thus far, this guide has discussed most of the major aspects of network operations automation. Chapter 1 discussed the essentials, including the benefits offered by automation. Chapter 2 focused on compliance and security, and how they can benefit from automation in network operations. Chapter 3 covered automation from the viewpoint of maximizing availability; this chapter touched on a very important aspect of automation—business processes. In addition, it outlined how factors such as a change assessment, a complete change management process, and other processes can help drive network operations automation more effectively. This chapter expands on that theme and discusses the need for business processes for *all* network operations, for finding a solution that helps implement that process, and for integrating the solution and your processes into a cohesive whole.

The idea behind this chapter is to create processes within your company that result in your network being managed and operated in a way that meets all your business needs. From that process, you'll evaluate technological solutions that allow that process to be realized—essentially, bridging the gap between what the business requires and what you could normally deliver, on your own, in terms of implementation. Once a solution is selected, you'll need to integrate it with your processes. Finally, because coming up with business plans can often be difficult (especially if you've never done it before), the chapter will look at sample business plans that cover tasks such as daily administration, auditing, disaster recovery, and so forth.

Building the Business Process

Too often, companies purchase technology solutions or implement new technologies without first fully defining the process that those technologies and solutions will support. It's a bad idea: Without knowing what you want to do, how will you know if you're doing it correctly? Fortunately, creating a process doesn't have to be difficult. Start by thinking about what your business really needs, then utilize a framework that helps provide a structure for your new process, essentially giving you a template, or head start.

By design, networks that are up and running *stay* up and running. The only time things tend to go wrong—and therefore require management—is when changes are made (apart from unforeseeable disasters or equipment failures, of course). Disaster recovery is also a concern, but again it tends to kick in when network devices are changed: That's when you need to, for example, make a new backup of the devices' configurations. Thus, although network operations processes *support* a variety of business needs—including availability, security, compliance, and more—they tend to *focus* on configuration and change management. That is precisely why you need a process. By managing change, you ensure that the network fulfills its primary purpose of delivering reliable communications between computers.

Frameworks for Change and Configuration Management

Currently, the most respected business process frameworks in the IT industry come from the Information Technology Infrastructure Library (ITIL), a product of the United Kingdom's Office of Government Commerce. OGC's job is to work with public (that is, government) organizations to help them improve their efficiency; ITIL is a major component of how OGC accomplishes that mission. ITIL is essentially a cohesive set of best practices, drawn from public and private sectors and codified into a complete IT management framework.

📖 You can learn more about ITIL at http://www.itil.co.uk.

The portion of ITIL that applies to network operations, the Service and Support segment, is available as a complete, standalone publication. This segment covers Service Desk management, Incident Management, Problem Management, Configuration Management, Change Management, and Release Management—with the latter three being the most important for network operations. Related segments include Service Delivery (which includes IT Service Continuity Management, Availability Management, and Capacity Management).

📖 The complete list of ITIL publications—they're all fascinating—can be found at http://www.itil.co.uk/publications.htm, where you can also place orders.

💣 Contrary to popular belief, the ITIL materials are not public domain in the usual sense of the term. Although they are widely available, they are copyrighted by the UK government, and that copyright is recognized under international copyright laws and agreements.

Notice that ITIL defines both *configuration* and *change* management. In the ITIL world, *change management* is the practice of "ensuring all changes to Configurable Items (CIs) are carried out in a planned and authorised [sic] manner. This includes ensuring that there is a business reason behind each change, identifying the specific CIs and IT services affected by the change, planning the change, testing the change, and having a backout plan should the change result in an unexpected state of the CI." Security and compliance, as business needs, are incorporated into the process, as part of "ensuring that there is a business reason."

Configuration management in ITIL is a complementary practice, defined as the "implementation of a database—Configuration Management Database, or CMDB—that contains details of the organization's elements that are used in the provision[ing] and management of its IT services. This is more than just an 'asset register,' as it contains information that relates to the maintenance, movement, and problems experienced with CIs."

Configuration management is much less of a *process* than change management; configuration management essentially consists of identifying managed assets for inclusion in the CMDB, controlling each asset (the change management process), recording the status of each asset in the CMDB, and periodically verifying that the CMDB is correct and up-to-date. Change management is where the real process-work comes in.

Examining Your Current Processes

First, you must understand how you *currently* do business. Take a moment to lay out your business processes for network operations *as they exist today.* This examination doesn't need to be fancy; a hand-drawn sketch is fine. Perhaps it'll look something like the sketch that Figure 4.1 shows.
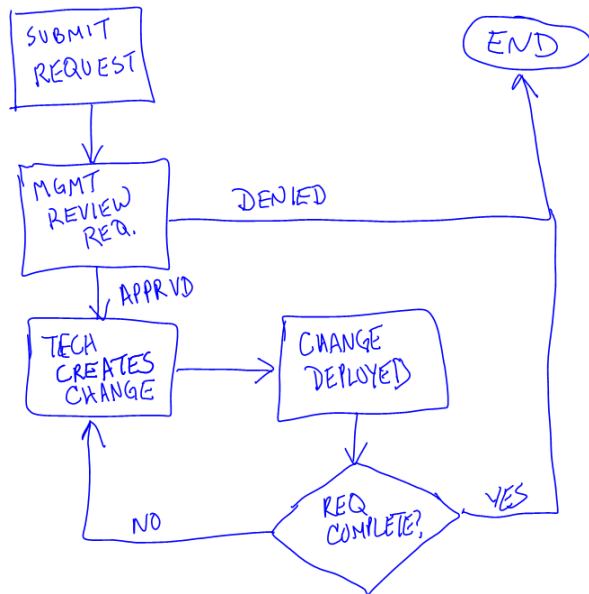
Figure 4.1: Current business process example.

This step is usually the best way to begin creating a new process because it gives you something to analyze and think about. Now you have something to start with and you can begin to identify areas where things will go wrong. For example, ask yourself whether the existing process incorporates the practices you think are needed. Using the process that Figure 4.1 show as an example, consider that following obvious weak points:

- The change isn't documented.
- There is no peer review of changes before they are implemented.
- Management has no input into the schedule of change implementation, meaning implementation may be unexpected or poorly communicated.
- Technicians can engage in an iterative process of changes until they feel they've completed the request; this process can lead to additional unnecessary downtime.
- Changes aren't archived and there isn't a process for rolling back changes that don't work out the way they are supposed to.
- Changes aren't prioritized or categorized, meaning that even important, urgent changes may be treated as longer-term changes.
- This process makes it seem as if network technicians keep most of their "documentation" in their heads rather than on paper or in a file where others can access it.

Analysis of what you actually have reveals the areas where improvement is needed. Begin adapting your business process to look the way you think it *should*, regardless of how or why you do things currently.

Adapting Your Processes

In addition to the weak points already pointed out, there are several missing elements in the existing process—you can probably spot additional things that you would like to see added, so do so. Pull out more paper or even an application such as Microsoft Visio, and start developing a process that meets your needs. As you go, make notations about where tools might be able to help. For example, if you add a step to "archive existing configuration" that happens before any changes are made, you might make a note to look for tools that can automatically archive your device configurations. For a "deploy change" step, you might look for tools that can automatically deploy changes consistently to multiple devices or even do so after hours when fewer users will be impacted. To enforce consistency, you might look for a tool that provides engineering templates.

One of the problems with many processes is that they don't accommodate the actual players in your environment. Creating a flowchart that identifies the roles—requestors, management, technicians, and so forth—can really help identify the people who are using and participating in this process. Figure 4.2 provides an example.
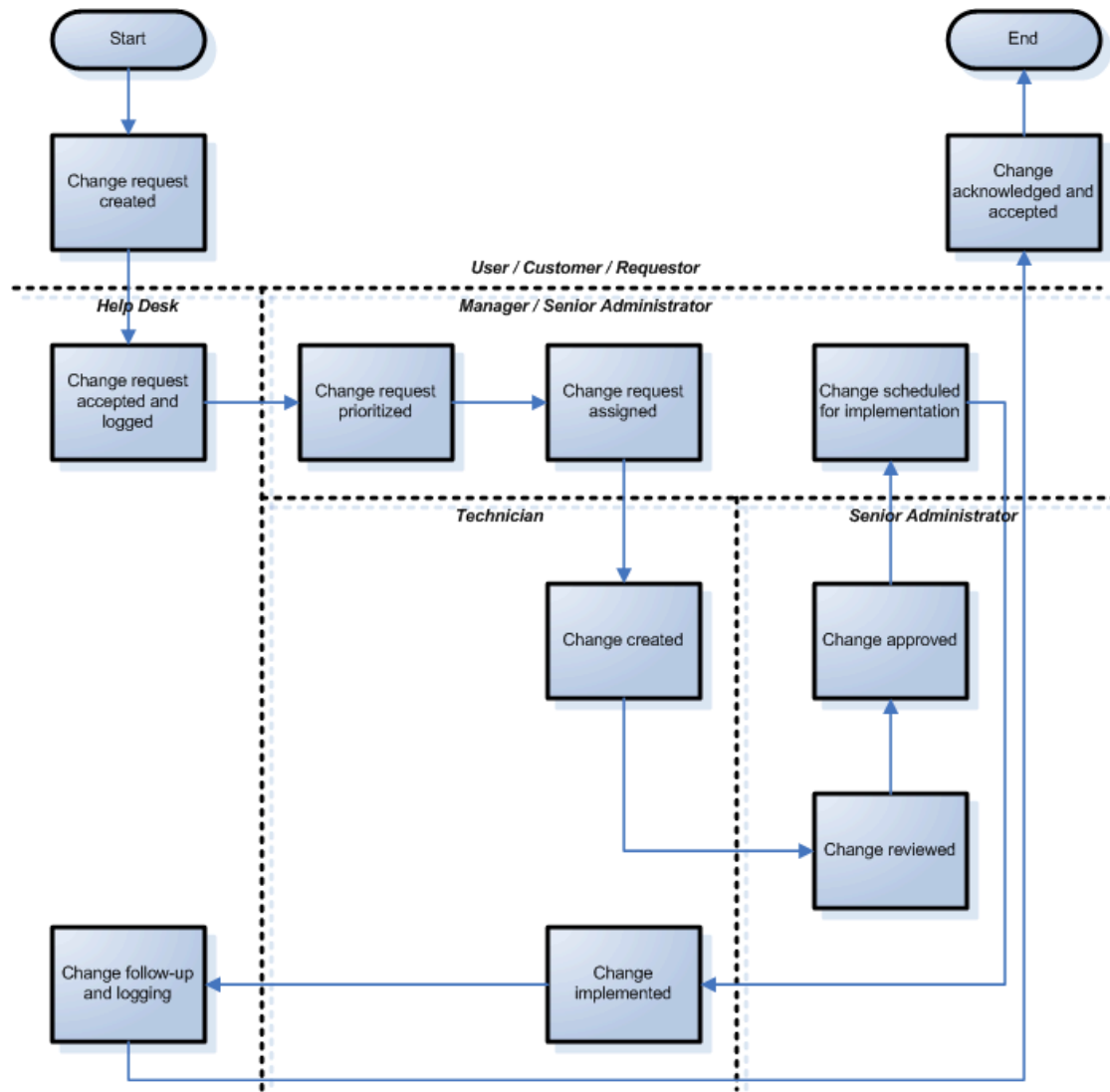
Figure 4.2: Process segmented by participant.

Although this type of flowchart might not be the most useful when it comes to ensuring a safe and reliable process, it can highlight unnecessary redundancies and bureaucracy in your project, giving you an opportunity to streamline the process if desired. For example, in the process that Figure 4.2 shows, the manager might include a tentative schedule with the request assignment. That way, when the peer review by the senior administrator is complete, the process could flow immediately back to the technician for implementation because the schedule has already been set—rather than flowing back to management for scheduling. An exception flow could be provided for changes that take too long to review and fix, making the schedule no longer feasible; such a revision would provide a more streamlined process for the majority of changes, while providing support for changes that can't be accommodated within the streamlining. So where does ITIL fit in? Let's take a look.

📖 You can learn more about building processes in this fashion in *Definitive Guide to Enterprise Network Change and Configuration Management* (Realtimepublishers.com).

The ITIL Connection

ITIL is designed to help produce efficient, error-free processes. Most major professional industries have sets of best practices. Accountants, for example, follow Generally Accepted Accounting Practices (GAAP), which are a set of best practices that have evolved over time. Attorneys also have best practices, as do doctors, nurses, and many other professions. IT, however, has evolved at such a fast pace that formal best practices haven't necessarily been forthcoming, or as formally documented as something like GAAP.

ITIL is essentially the current closest thing the IT industry has to GAAP: ITIL are a set of documented best practices that come from the industry's long experience with IT management. Like GAAP, they're not laws or hard-and-fast rules but rather a set of common guidelines that have worked for a number of IT organizations over a long period of time. Using ITIL, like using GAAP, isn't guaranteed to keep you out of trouble, but you're a lot less likely to encounter problems in your IT infrastructure by implementing the practices set forth in ITIL.

An ITIL-compliant process will include some of these major elements:

- Change logging and filtering—In this step, Requests for Change (RFCs) are evaluated for necessity and categorized into major- and minor-impact changes. Changes are reviewed by a Change Advisory Board (CAB), and, in the case of major changes, by an executive committee (EC). The purpose of this step is to figure out which changes are important and which ones carry a great deal of risk.

- Managing changes and the change process—This area incorporates the actual building of the change, peer review, implementation and schedule, and so forth. A number of communications processes are necessary at this stage to keep the organization working smoothly through the change.

- Reviewing and closing RFCs—This functional area is a chance to look back and review changes for mistakes, documenting anything that can be used to improve future change efforts. This sort of "post-mortem" exercise is an opportunity to evaluate RFCs' original intent with the final outcome, and is an important contributor to the auditing process.

- A backout plan—This plan enables the ability to roll back changes that don't work as expected, to minimize negative impact on the environment.

ITIL Terminology

Reading through the ITIL documents and related information on the Web can be an exercise in jargon. The reason, in part, is the result of the many specialized terms and acronyms used in ITIL and, in part, because the original documents were developed in the UK, where the language is slightly different than American English. Some of the general terms you'll need to keep in mind include:

- Request for Change (RFC)—A formal document detailing the change that is requested.

- Document—ITIL recognizes that electronic documents—email, word processor files, and database entries—are easier to manage than paper documents in all but the smallest IT shops.

- Change Advisory Board (CAB)—Comprised of major IT department managers, senior users, and a managing change manager.

- Executive committee (EC)—A subset of the CAB that reviews urgent changes without convening the entire CAB; consists of the change manager and service level managers.

- Change manager—The executive in charge of controlling and managing all change within the organization; heads the CAB and EC.

- Configuration item (CI)—Any device, software application, or other configurable entity that falls under change and configuration management (for example, router, firewall, access control list—ACL, host file, and so on).

- Service Level Agreement (SLA)—A set of standards defining IT quality and service targets; includes maximum downtime goals, response time goals, and so forth.

- Service level managers—IT managers who manage their operations to company-defined SLAs.

- IT Planning Secretariat (ITSP) and IT Executive Committee (ITEC)—In the United States, these roles essentially correspond to "upper IT management." If a specific group of IT managers is responsible for planning, such as a group of business process analysts, they would be the ITSP. The roles primarily come into play for reviewing and planning major-level changes that deeply impact the entire environment, such as re-architecting an entire network or deploying a major new enterprise application. The real contribution of these roles is to maintain a healthy sense of the business needs and impacts while reviewing RFCs.

The OGC maintains an ITIL glossary online at http://www.ogc.gov.uk/index.asp?id=1000369; this online glossary is a useful reference for any unfamiliar terms you come across.

Figure 4.3 shows a sample ITIL process that you can modify to meet your organization's specific needs. This process includes all the key elements of an ITIL-inspired process, including a CAB/EC review, change categorization, risk analysis, change development and testing, notification, implementation, auditing and documentation, and so forth. These key elements help to ensure that changes meet a business need, they cause a minimum of disruption, and they're fully tested and documented, preferably in a CMDB of some kind.
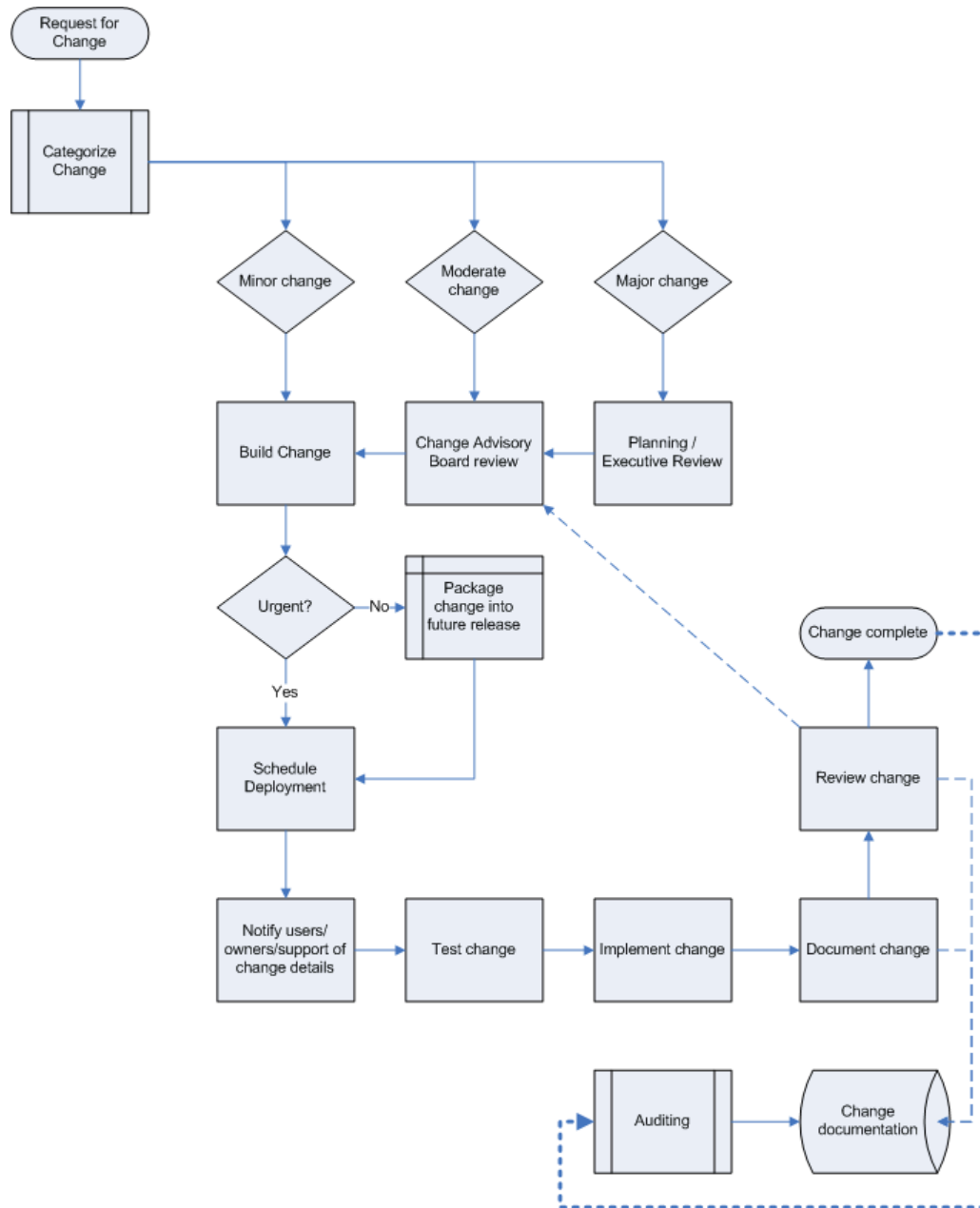
Figure 4.3: Sample ITIL-compliant process.

> ✎ This particular example is not complete: It doesn't include backups that would provide for a backout plan if a deployed change didn't work out. That's okay; this is just an example, and it isn't meant to be complete yet.

Of course, having a process such as this is just the beginning—it's useless without some kind of tool or solution that implements the process, enforcing it and handling the portions of the process that can't practically be completed manually. *That's* where a network operations automation solution comes into play.

From Process to Reality: Where Automation Fits In

The process that Figure 4.3 shows is one many companies probably wouldn't mind, except that it carries several unrealistic, or at least impractical, elements. For example, is it practical to have *every single change* reviewed by a committee? Is it realistic to *enforce* a process like this in a manner that prevents technicians from simply becoming annoyed at the process itself and bypassing it?

That's where automation fits in. In fact, you really can't have a robust, reliable operations process without some kind of automation solution, because without automation, too much of the process would require manual, impractical effort—and be too easily bypassed. For example, let's consider how automation solutions might help with the process that Figure 4.3 shows to make it more practical, more realistic, and more reliable:

- Change categorization could occur in a Help desk ticket-tracking system, allowing changes to be more easily reviewed, categorized, and assigned to a technician for development. High-priority changes would be tagged as such in the system, allowing faster review by a subset of the normal reviewers (that's what the EC is for). Help desk systems already support this kind of prioritization.

- Change building and scheduling can be handled by a network configuration management system that supports configuration templates, scheduling, and deployment. These systems might also provide built-in workflow support for change reviewing and approval, thereby encompassing the majority of the process right within one tool and eliminating unauthorized changes.

- Configuration management systems are often built around a CMDB, giving you an automated documentation system that keeps track of changes to devices.

In fact, the right thing to do at this point in your plan is to tag your business process flowchart with notes, indicating where some kind of tool would be needed to help facilitate or enforce various parts of the process. That way, you'll have a clear idea of what capabilities a solution will need to suit your environment. Figure 4.4 shows a sample process with automation notes added (note that, for space considerations, this is a simplified process flowchart).

This flowchart's notes include desires for specific functionality: Enforceable change review workflow, automated backups, centralized scheduling, and so forth. These are often *technical* requirements more than business requirements; things you need the technology to do in order to make your *business* process more feasible. Those are great notes to make at this time, as they'll all coalesce into a set of firm requirements for a technology solution.
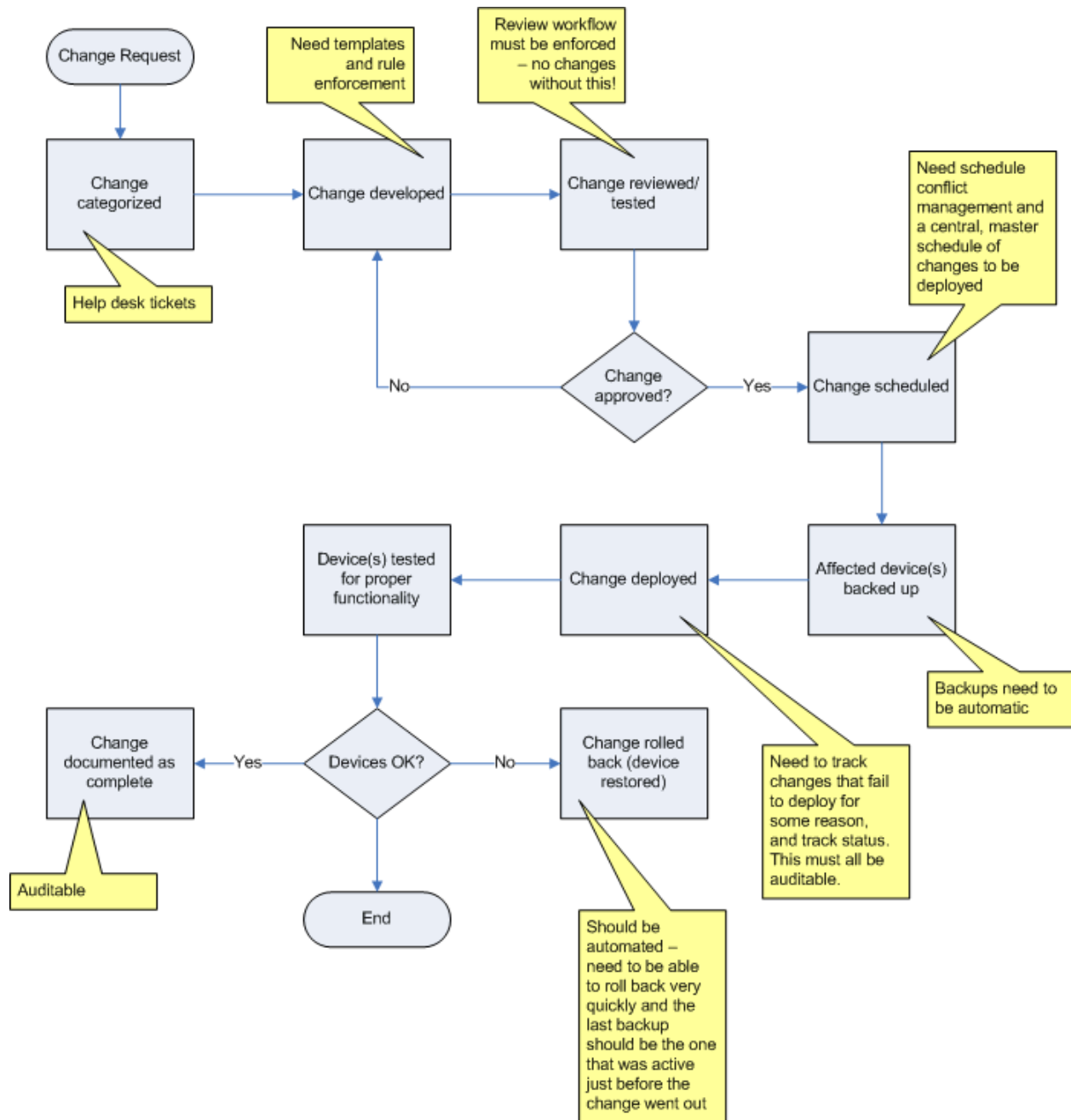
Figure 4.4: Noting automation requirements in your business process.

The bottom line is this: If you're going to automate network operations and realize all the benefits of automation, you need a plan. That plan is built from a business process, but that business process can't often be fully implemented or enforced until you've got a tool capable of doing so for you. Thus, if you want to automate your network operations, you need a tool that will do it for you. That's not a big deal, because there are dozens, if not hundreds, of tools on the market. The trick is finding the one that supports your process—because technology solutions should *always* accommodate your business, not the other way around.

Creating a Solution Evaluation Project

Evaluating software products is one of my least-favorite jobs, primarily because so many of the companies I've worked with in the past make it such a difficult, frustrating process, fraught with internal bickering and political concerns. Unfortunately, I can't help make those aspects of a solution evaluation better. However, I can help with the actual technical piece by providing some examples and suggestions that are common to almost all network operations automation needs, essentially giving you a head start in your evaluation—perhaps allowing you to move faster than your organization's naysayers and political infighters, finishing your evaluation before they've even realized it's underway.

Determining Critical Criteria

The first step is to determine what you need the solution to do. I like to start with a feature comparison chart, similar to the one that Figure 4.5 shows, in which I can list all the features and capabilities I want the solution to have.

Network Automation Solutions - Evaluation

	Product A	Product B	Product C	Product D	Product E	Product F
Auto-backup						
Approval workflow						
Customizable workflow						
Configuration rules						
Notify on broken rule						
Auto-remediate on broken rule						
Allows full Telnet/ SSH access						
Secure config repository						
Built-in compliance audit reports						
Integrates with LDAP for authent.						

Figure 4.5: Example evaluation form

Where do the features come from? From your business process. Spend some time with everyone who uses or is affected by that process and sort out exactly what kind of capabilities you want a solution to have in order to support that process. That's not saying you'll find a solution that meets every one of your requirements, but now's the time to essentially make a "wish list" of everything the perfect solution will do. The following list highlights some ideas to get you started:

- The ability to integrate with your authentication mechanism. In the example in Figure 4.5, I listed this as integrating with an LDAP directory; alternative requirements might include authentication tokens such as SecurID, or you might be perfectly happy with the RADIUS or TACACS+ authentication that you already use.

- The ability to integrate or work with your Help desk ticket-tracking system. This integration doesn't need to be fancy, maybe just the ability in the automation system to enter a Help desk ticket number, thereby tying a change to a ticket.

- The ability to set up a custom workflow for change review and approval, including designating who can submit changes, approve them, and who should be copied on the change notices.

- Granular security, allowing you to give individuals—on a role-by-role basis—access to only the bits they need to do their job. For example, auditors may need the ability to look up, but not change, device configurations.

- The ability to schedule changes for deployment.

- Deployment tracking so that you can see which devices successfully receive a change and which don't.

- For failed deployments, per-device details about what went wrong, ideally with suggestions about how to fix it.

- The ability to define groups of devices so that deploying changes to similar or related devices as a group is easier.

- Schedule conflict tracking so that if someone submits a change that will affect the same device as another scheduled change, notify everyone involved so that they can figure out if any conflicts exist and what to do about them.

- The ability to define rules that describe how a device should be configured:

  - The ability to analyze devices for compliance with the aforementioned rules and alert you (or create reports) of problem devices.

  - The ability to automatically deploy changes in order to remediate devices that aren't complying with the aforementioned configuration rules.

- A secure configuration repository that can be easily backed up to offline storage for safekeeping.

- The ability to provide direct device access (Telnet or SSH) while maintaining a keystroke log of all device interactions.

- No single point of failure—the solution should be built in such a way that a failed server won't prevent you from using the solution entirely.

- One-click (or at least very few clicks) rollback of a device to a previous configuration.

- Automatic backup of device configurations.

- Ability to detect possible changes by analyzing Syslog, TACACS+, RADIUS, SNMP, or other technologies and using those as alerts to log in and pull the device configuration.

- Side-by-side comparison of device configuration versions with difference highlighting.

- Support for any device on your network and an architecture that allows new device support to be added without the vendor having to release a major new version of the product.

- Built-in reports for anything you've identified a need (this is the thing you're least likely to get, since many reports are very company-specific, but it doesn't hurt to be on the lookout for it).

- The ability to create ad-hoc reports and to define your own reports.

The list goes on. If your feature comparison list isn't several pages long, then you're 'not trying hard enough: This is your only chance to ask for features, so get 'em all in there.

> ☞ Remember, adding notes to your business process can be the best way to identify specific business requirements. Those notes can then become specific features in your evaluation.

Evaluating Solutions

Engage vendors to help you evaluate their solutions. Have your criteria list in hand when you do so. If the vendor wants to point out additional features that you've not considered—they will, salespeople can't help themselves—that's great; note them down separately. If you haven't listed the feature, it might not be important to you, but it might still serve as a tiebreaker later on.

Be sure you know *exactly* what you want from each feature you've listed. If necessary, write up a short paragraph explaining what you need the feature to do, and evaluate solutions for their ability to do *what you want.* Often, these automation solutions are complicated enough that you can't simply install them yourself in a lab to check them out; you may be relying on vendor-led demonstrations, instead. There is nothing wrong with that, provided that you're driving the show. When a solution offers a feature that doesn't *quite* do what you wanted, make detailed notes about what it *does* do. It's possible that the competition will do things the same way and that you won't be able to get exactly what you want, so it's important to understand what you *can* get. It's also important to understand *how* various features are supported—ask for a demonstration, if possible, so that you can *see* features in action.

Anytime you hear an answer like "We're adding that in the next version," get it in writing. You need to recognize that network automation is a rapidly evolving and highly competitive field;

vendors frequently *do* add major functionality in new versions. But don't base your evaluation on that promise unless the vendor can make the promise in writing and really commit to it.

Scoring Evaluations

Scoring evaluations can be tricky. After all, some features will be deal-breakers for you if they aren't available, and others are just "nice to have" features that you can, ultimately, live without. To help reflect this reality, I use a two-part scoring system. First, for each feature, I define an importance, on a scale of 1 to 3, with 1 being "nice to have" features and 3 being "absolutely required" features. Figure 4.6 shows my evaluation form modified to list these values.

Network Automation Solutions - Evaluation

	Product A	Product B	Product C	Product D	Product E	Value
Auto-backup						3
Approval workflow						3
Customizable workflow						3
Configuration rules						2
Notify on broken rule						2
Auto-remediate on broken rule						1
Allows full Telnet/ SSH access						2
Secure config repository						3
Built-in compliance audit reports						2
Integrates with LDAP for authent.						1

Figure 4.6: Identifying importance values for each feature.

If a product is missing a "got-to-have" feature, it is off the list. That narrows the field. Then, when evaluating each solution, I give it a score based on how well it implements each feature I want. I tend to make notes detailing why I gave each score so that I can better understand the differences between solutions. I usually use a scale of 0 (feature not implemented) to 3 (feature implemented exactly as I wanted), but you can use a scale of 0 to 5 or whatever you're comfortable with. Figure 4.7 shows the evaluation form with a couple of products' scores filled in.

Network Automation Solutions - Evaluation

	Product A	Product B	Product C	Product D	Product E	Value
Auto-backup	2	3				3
Approval workflow	1	3				3
Customizable workflow	0	2				3
Configuration rules	0	3				2
Notify on broken rule	0	3				2
Auto-remediate on broken rule	0	2				1
Allows full Telnet/ SSH access	3	2				2
Secure config repository	2	2				3
Built-in compliance audit reports	3	2				2
Integrates with LDAP for authent.	0	1				1

Figure 4.7: Scoring evaluated products.

Then, I simply multiply my "importance" value by the product's score, for a total weighted score. Products doing a great job with features I really need get a very high weighted score; products that do a great job with features I don't care about as much get a lower score. The final sum of all weighted scores will help me identify the best product. Obviously, minor score differences between products will require a closer look, but this exercise is useful for eliminating

products that simply don't do a good job with the most important features. Figure 4.8 shows the completed form for two products, with weighted scores shown (the format I used is score/weighted score).

Network Automation Solutions - Evaluation

	Product A	Product B	Product C	Product D	Product E	Value
Auto-backup	2/6	3/9				3
Approval workflow	1/3	3/9				3
Customizable workflow	0	2/6				3
Configuration rules	0	3/6				2
Notify on broken rule	0	3/6				2
Auto-remediate on broken rule	0	2/2				1
Allows full Telnet/ SSH access	3/6	2/4				2
Secure config repository	2/6	2/3				3
Built-in compliance audit reports	2/6	2/4				2
Integrates with LDAP for authent.	0	1/1				1

27   50

Figure 4.8: Completed, weighted evaluation.

Obviously, this process can be time-consuming when you're working with several pages of criteria; however, this decision is an important one for your business, and it's worth the time to

understand how different products can help you solve your needs. This evaluation methodology will help you keep your eyes on the needs of the business and help ensure that the solution that best implements the features you need the most will rise to the top of your evaluation project.

Integrating Your Processes and a Solution

One you've selected a solution, you have to start using it. That probably sounds obvious enough to be ridiculous, but most companies who implement a network automation solution don't fully utilize it. Perhaps they'll use the obvious features, such as automatic device configuration backups and configuration change deployment, but you need to look back at your business process and make sure that every bit of it that *can* be automated *is* being automated.

For example, if the solution you've selected supports the creation of configuration rules, take the time to create them. Make a rule for each and every aspect of your devices' configurations that you possible can, if for no other purpose than to allow your automation solution to show you which devices aren't configured according to the rules. Decide which configuration settings you feel comfortable turning over to automated remediation, if your solution supports it: Having SNMP community strings automatically configured, for example, is fairly low-risk and will help you gain confidence and experience with your new solution.

Look at everything your new solution is capable of doing and decide where those features might fit into your business process. Automate *as much as possible.* Remember, automation equals more efficiency, more consistency, more security, and more flexibility for your network and your business. *Use* that automation to the maximum degree possible.

Create and distribute process flowcharts that specifically reference your solution's functionality. Figure 4.9 provides an example: Notice that this process isn't massively different than the earlier one, but it now indicates which process steps take place within an automation solution. This is a flowchart every network administrator and technician should have readily available so that they can see which parts of their jobs are now performed within your new solution. Fully integrating the solution into your business processes in this fashion is the best way to use the solution to its fullest potential.

Obviously, how your process and solution integrate will depend on your process and the solution you select. In the figure, purple boxes indicate the portions of the process that occur within, or are handled by, the automation solution; notes provide details about how the solution handles each step. This particular solution offers templates and configuration rules to assist with change development and provides a workflow that allows changes to be reviewed and approved. Only changes that are approved can enter the solution's deployment schedule, and the solution handles deployment automatically. Affected devices are backed up automatically, and can be restored if the change doesn't go as expected.

The chart in Figure 4.9 shows a very effective way of seeing how much an automation solution can contribute to a network operation's process. Nearly every major aspect of change and configuration management is automated in some fashion, and the solution provides a means for enforcing this workflow.
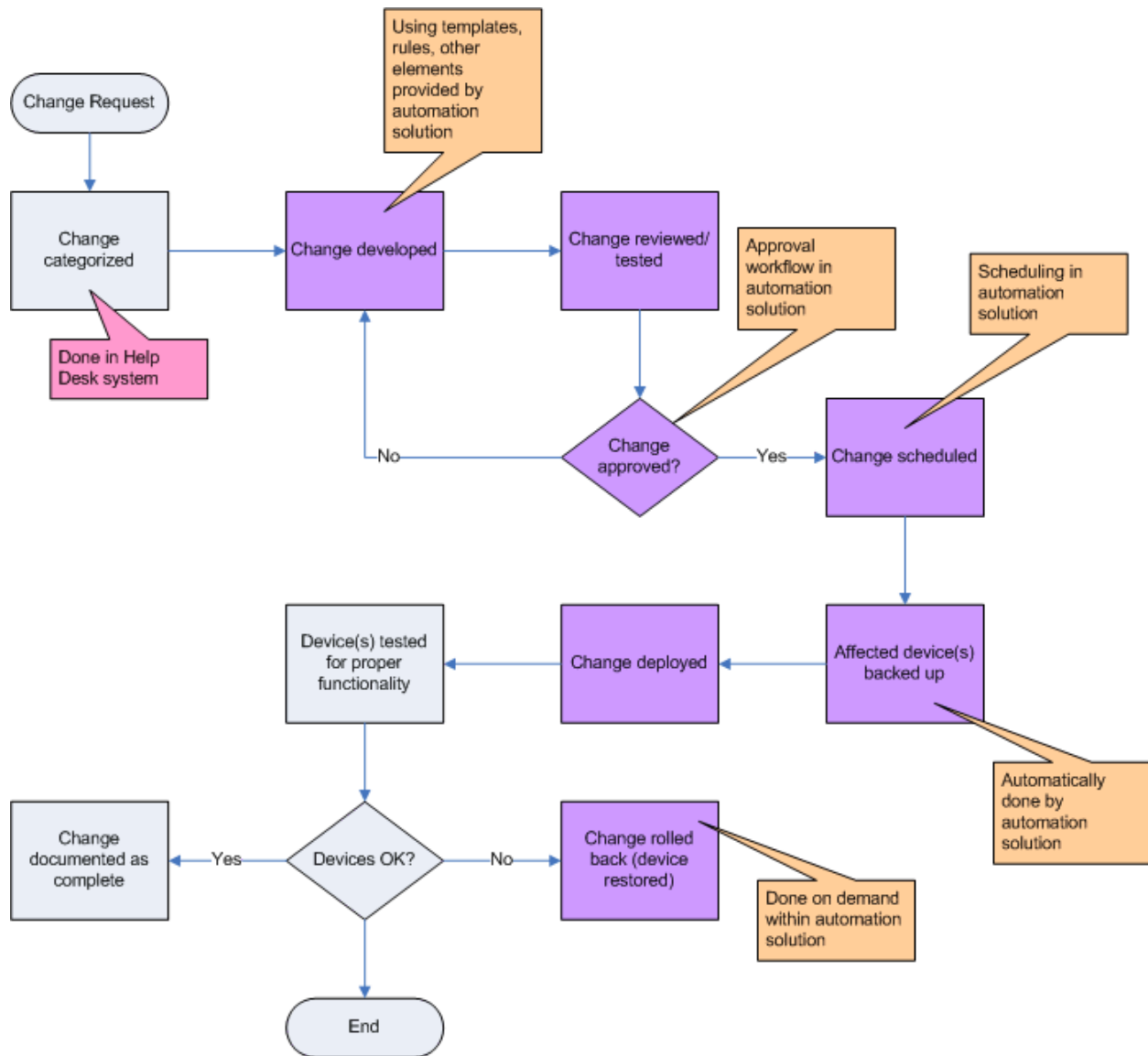
Figure 4.9: Integrating your solution into your process.

Creating Business Plans

Creating business plans can be difficult, especially for factors as prosaic as daily network device administration. The problem is that it's sometimes difficult to really pin down the steps in the process: "I log in, I make the change, I log out" might not seem like much, but you can certainly draw a flowchart for it. That flowchart—simplistic as it is—will highlight the holes in that process, and allow you to clearly see what business needs aren't being met. *That* is the big reason for drawing flowcharts in the first place: To graphically illustrate the business needs that aren't being met.

To get you started, the following sections present sample charts for various tasks, including daily administration, auditing, and disaster recovery as well as how they link in to one another. These processes are also ITIL-inspired, which means they incorporate many of the best practices documented in ITIL, although in places I may use simpler terminology (such as "change review" rather than "change review by the CAB/EC"). The goal of these examples is to simply make process illustrations of best practices, which you can then adopt and adapt as needed.

Planning for Daily Administration

Daily administration primarily deals with changes to device configurations, whether those changes are to support new business requirements or to fix problems that have occurred. Typically, organizations try to schedule changes—especially ones that enable new functionality—for scheduled maintenance periods; changes that fix a problem may be implemented on a more ad-hoc basis. Regardless, all changes should go through some kind of "daily administration" process, such as the one Figure 4.10 shows.

Figure 4.10: Example process for daily administration.

Notice that this process includes an accommodation for out-of-process changes. In this example, the process is to roll back the unauthorized change, thus ensuring that no changes occur outside this process. Also note that this process doesn't focus on the *how* of developing and deploying changes; that's something you'll want to think about for your solution evaluations, however. For example, you may want a solution that allows changes to be developed in a template-driven graphical user interface (GUI) or allows administrators to use familiar tools such as Telnet to reconfigure devices or generate configuration scripts. This example business process supports any of these implementation means; you simply need to select a solution that provides the right toolset for your organization. Notice, too, that the "Change Reviewed" step includes *any* reviews

that are necessary—including peer reviews, automated reviews against any policies or rules you've created, and so forth.

Planning for Auditing

Figure 4.11 shows a revised process that includes business requirements for auditing. Typically, you're going to look at an automation solution to provide the logging capabilities shown in this figure.
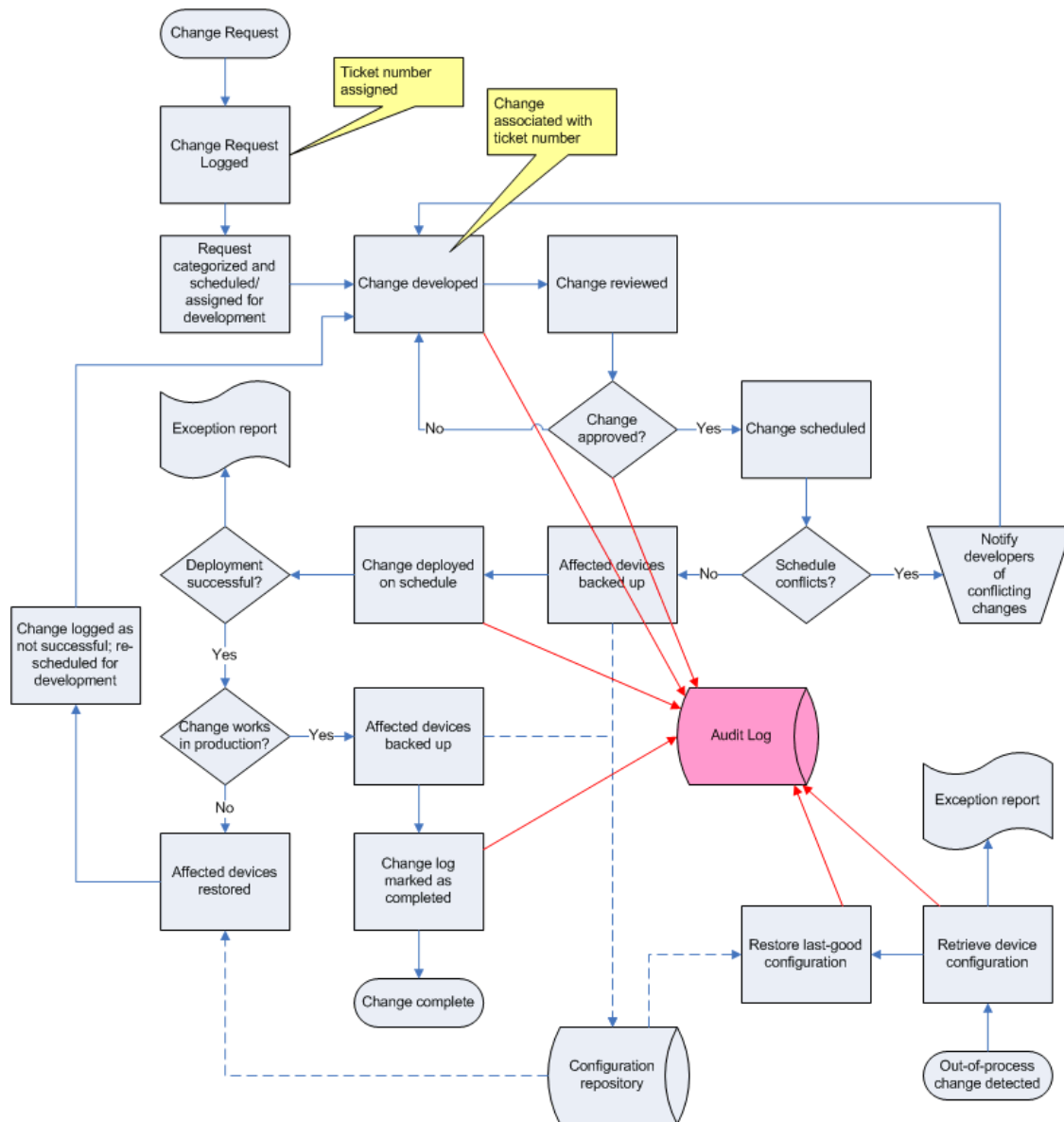
Figure 4.11: Including auditing in your business process.

Looking at this process, you know that you need the automation solution to generate appropriate auditing information at certain points—when changes are developed, approved, deployed, rolled back, and so forth. By linking a change to a Help desk tracking system (for example), you can show a complete life cycle (from request to completion) for each change, proving that the change

actually went through the process (process compliance is a big consideration for auditors). This auditing flowchart isn't so much a process as it is a set of requirements, helping you to select an automation solution that provides logging capabilities that comply with your auditing needs and requirements.

Planning for Disaster

An effective business process for daily administration will have built-in disaster recovery. Take a look at Figure 4.12, which highlights—in yellow—the aspects of this process that lend themselves to disaster recovery. Also notice the pink highlight, which is a part of the process that helps support business continuity.
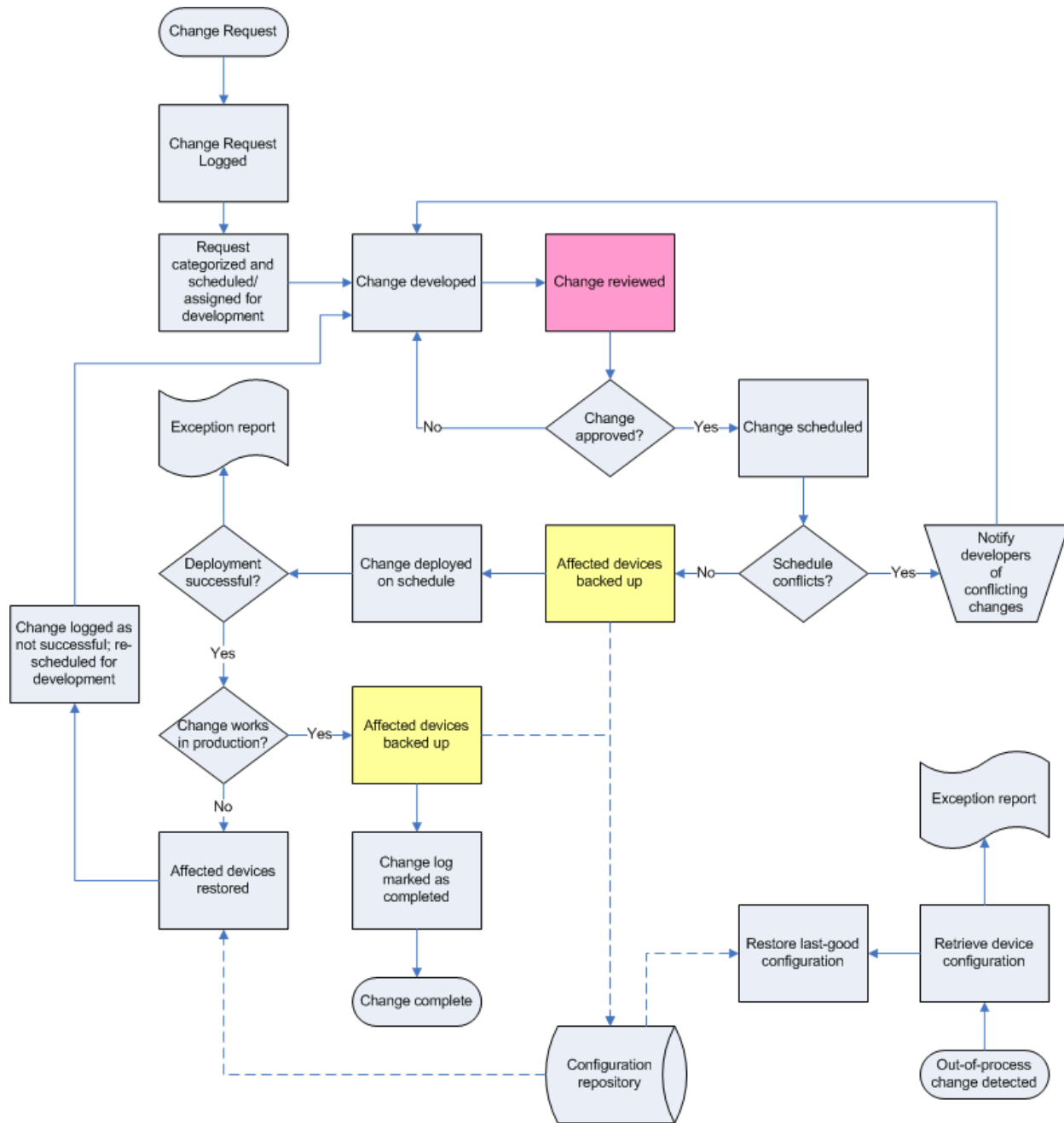
Figure 4.12: Disaster recovery and business continuity support in a robust process.

By creating a backup of device configurations before changes are deployed, as well as after changes are successfully deployed, you're assured of having the latest and greatest configuration in a repository should disaster occur and require restoration. Helping to prevent disaster (at least disaster through misconfiguration) is this process' change review and approval requirement. By reviewing changes, wrong ones are less likely to be deployed, thus providing better business continuity.

Summary

This chapter has focused on the need for a comprehensive plan for network operations automation. Simply buying tools won't work; you need to have clear business goals, which allow you to select a technology solution that will meet those goals. The way to establish your goals is simply to create a reliable business process that meets all your business needs, then select a solution that can help automate, enable, and enforce that business process. This chapter has shown you several business processes that meet various needs for daily administration, auditing, disaster recovery, and so forth; these are all common business needs that any valid business process needs to address. They're also considerations that a properly selected automation solution can provide for you.

As this is the end of this guide, it's worthwhile to briefly review the main points of the previous chapters. First, automated networks are highly desirable from a business point of view. They're easier to configure and more consistently configured, which makes them more reliable, than manually administrated networks. They're also easier to recover in the event of a disaster and, perhaps most importantly, they're easier to secure, make compliant with legislative requirements, and easier to audit. These three factors alone can almost make an automated network worth any price! Automated networks are also more efficient because you spend less time managing them and dealing with problems. Finally—and this is too often overlooked—automated networks are more flexible. They're able to evolve and change more quickly, more easily, and with less risk to meet new business requirements and keep the business competitive.

The benefits of automation are very clear when it comes to security and compliance. Automated networks can be configured to automatically detect, report, and even roll back inappropriate changes, helping to sharply reduce (if not eliminate) insecure, non-compliant configuration settings. This benefit is enormous to any business concerned about security or dealing with legislative compliance requirements because maintaining a secure and compliant environment would otherwise require tremendous manual effort—and industry experience suggests that a manually configured network is almost never fully secure and compliant. Automation can help avoid overlooked devices and can ensure that device configurations remain consistent. Automation can pick up where point-in-time auditing leaves off by *continuously* auditing devices and not allowing a misconfigured device to go unnoticed for any significant period of time. Automation can also make auditing easier by exposing auditing information quickly and clearly rather than forcing you to laboriously assemble these reports by hand.

Automation also has obvious benefits for high availability. Automation can ensure that your device configurations are always backed up and safe and can make it easy to quickly restore devices or to provision new devices as replacements to failed ones. Automation solutions provide a central CMDB that provides version-controlled storage for device configuration files, keeping them safe, accessible, and easily managed. An automation solution can help quickly recover from device failures, device misconfigurations, facility failures, and more. In addition, automation solutions can often *prevent* problems such as misconfiguration by enforcing known-good configuration templates, enforcing change review and approval workflows, and other elements that help ensure only proper changes are deployed to production.

Finally, as this chapter has explored, automation can make a "best practices" business process for network operations practical and realistic. Many best practices simply aren't achievable without unacceptable manual labor requirements—unless you automate them. Understanding your business requirements up front, then selecting a solution that meets those requirements, will help ensure that you get a network that is fully automated, highly flexible, as secure and compliant as possible, and fully in sync with your business needs.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.