



realtimepublishers.com[®]

The Definitive Guide[™] To

Enterprise Network Configuration and Change Management

VOYENCE[™]

Don Jones

Chapter 7: Network Configuration Management Best Practices	135
ITIL	135
About ITIL	136
ITIL Change Management	137
Change Logging and Filtering	140
Managing Changes and the Change Process	144
The CAB	149
Coordinating Change	150
Reviewing and Closing Requests for Change	151
Auditing and Management Reporting	152
ITIL Configuration Management	153
Identification	154
Control	154
Status	154
Verification	154
Assessing Your Practices	154
Assessing Your Change Filtering Process	155
Assessing Your Change Implementation Process	155
Assessing Your Change Review Process	156
Scoring Your Results	156
Summary	157

Copyright Statement

© 2004 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

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

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

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

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

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

Chapter 7: Network Configuration Management Best Practices

In the previous six chapters, I've spent a lot of time discussing what works and what doesn't when it comes to network configuration management. I've shown you various processes that you might adopt or modify and begin using in your environment. I've explained some of the underlying technologies that support automated configuration management, and I've discussed different categories of tools that you might be interested in to help automate configuration management in your environment. In this chapter, I'll introduce you to the IT industry's best practices for change and configuration management, and help you understand how they apply more specifically to change and configuration management in network devices.

ITIL

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 been forthcoming.

ITIL is essentially the IT industry's 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.

ITIL and GAAP

You can draw some interesting parallels between ITIL and GAAP. GAAP, the set of best practices used by accountants, is simply a set of practices that everybody more or less agrees on as being accurate. They're not laws or formal rules, and they don't cover every given situation. But they're a good idea, and accountants who stay well within the guidelines established by GAAP have a better chance of winning an audit or accounting review, simply because everyone agrees that GAAP is the right way to do things.

We in the IT industry haven't been subject to the kind of intense scrutiny that accountants are. However, the situation might be changing. Security, service availability, management, and other IT aspects can all have a major impact on IT operations and on businesses that rely on IT. It is becoming more common for IT managers to be formally "called to the carpet" to explain costly downtime, security breaches, and so forth. In the past, such incidents might have earned the wrath of a director or even the company CEO; today, it might gain the attention of shareholders and even government regulatory agencies. In fact, many aspects of IT management are already gaining regulatory recognition.

About ITIL

ITIL is the only comprehensive set of documentation for best practices in the IT industry. Originally published as a set of best practices books by the British Office of Government Commerce (OGC), ITIL has been adopted by a number of companies and organizations across the world. In the United Kingdom, ITIL books can be purchased directly from the government's Stationery Office; outside the UK, a number of independent publishers have licensed the rights to reproduce the ITIL books.

ITIL is organized into several major publications:

- **Software Asset Management**—This ITIL publication focuses on the management of corporate software, recognizing that software is one of the most critical aspects of IT.
- **Service Support**—This publication focuses on ensuring that users have access to the IT functions and services they need to do their jobs. This publication incorporates configuration and change management best practices, as those two functions play heavily into the availability of systems and services.
- **Service Delivery**—This publication focuses on providing support to the business and its users, including capacity management, financial management, service level management, and so forth.
- **Infrastructure Management**—This publication covers the creation of network and communications systems, their maintenance and management, and so forth.
- **Application Management**—This publication focuses on the life cycle of software applications and is intended as a guide for developers and service managers on how applications can be managed more effectively.
- **Security Management**—This publication looks at security and its relation to IT, and focuses on the process of implementing and maintaining security in the IT environment.

The concepts and processes in ITIL are non-proprietary, so you are free to use them however you choose within your organization. Borrow from them, adopt them wholesale, or simply use them as a guide to improving your existing processes.



There is no formal certification process for proving that you're ITIL-compliant, although a number of consulting companies offer services that they claim will ITIL-certify your organization. The OGC has several individual-level certifications designed to demonstrate a person's knowledge and experience with ITIL; there are no organization-level certifications along the lines of ISO9001.

On the OGC Web site (<http://www.ogc.gov.uk/index.asp?id=1000368>), OGC notes that it is waiting for the forthcoming BS15000 standard, which will incorporate aspects of ITIL. This standard is being produced by BSI (<http://www.bsi-global.com>), which serves as the National Standards Body of the UK.



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.

There are several places where you can learn more about ITIL in general. Two useful resources are:

- The official OGC site on ITIL starts at <http://www.ogc.gov.uk/index.asp?id=1000367>.
- The ITIL Directory is located at <http://www.iti-itsm-world.com>.

Be cautious, however, about simply searching Google for “itil.” Several consulting companies, unaffiliated with OGC, have domain names that include ITIL and go out of their way to look like “official” ITIL Web sites. ITIL publications should run about \$150 to \$200, so if you’re being asked to pay more than that, or being asked to buy them in a package with consulting services, read the fine print carefully.

For this chapter, I’m going to focus entirely on two aspects of ITIL: change management and configuration management. ITIL has very specific definitions for those terms, and defines different processes and activities for them. Although separate, change and configuration management are complementary aspects of IT management.



My goal in this chapter isn’t to parrot ITIL or provide you with a complete education in its principles and processes. Instead, I’m distilling the ITIL processes relevant to network device configuration management, and showing you how these processes work in an actual, production-level environment. Where possible, I’ll simplify more complex or abstract ITIL concepts to keep them on a relevant, working level.

ITIL Change Management

Although many sources tend to use the terms interchangeably, ITIL makes a distinction between *change management* and *configuration management*. In this section, I’ll focus on change management; I’ll cover configuration management later in this chapter.

ITIL defines *change management* as a means of controlling all changes that occur within the IT environment. These changes might include updates to software applications, configuration changes to network devices, redesign of the network infrastructure, or even something as simple as changing a backup and restore schedule. The ultimate goal of change management is to accomplish all changes without errors or wrong decisions, so changes never create a negative situation (such as downtime) and there is never a need or reason to roll back or undo a change that has been made.

Figure 7.1 illustrates a simplified version of the ITIL change management process.

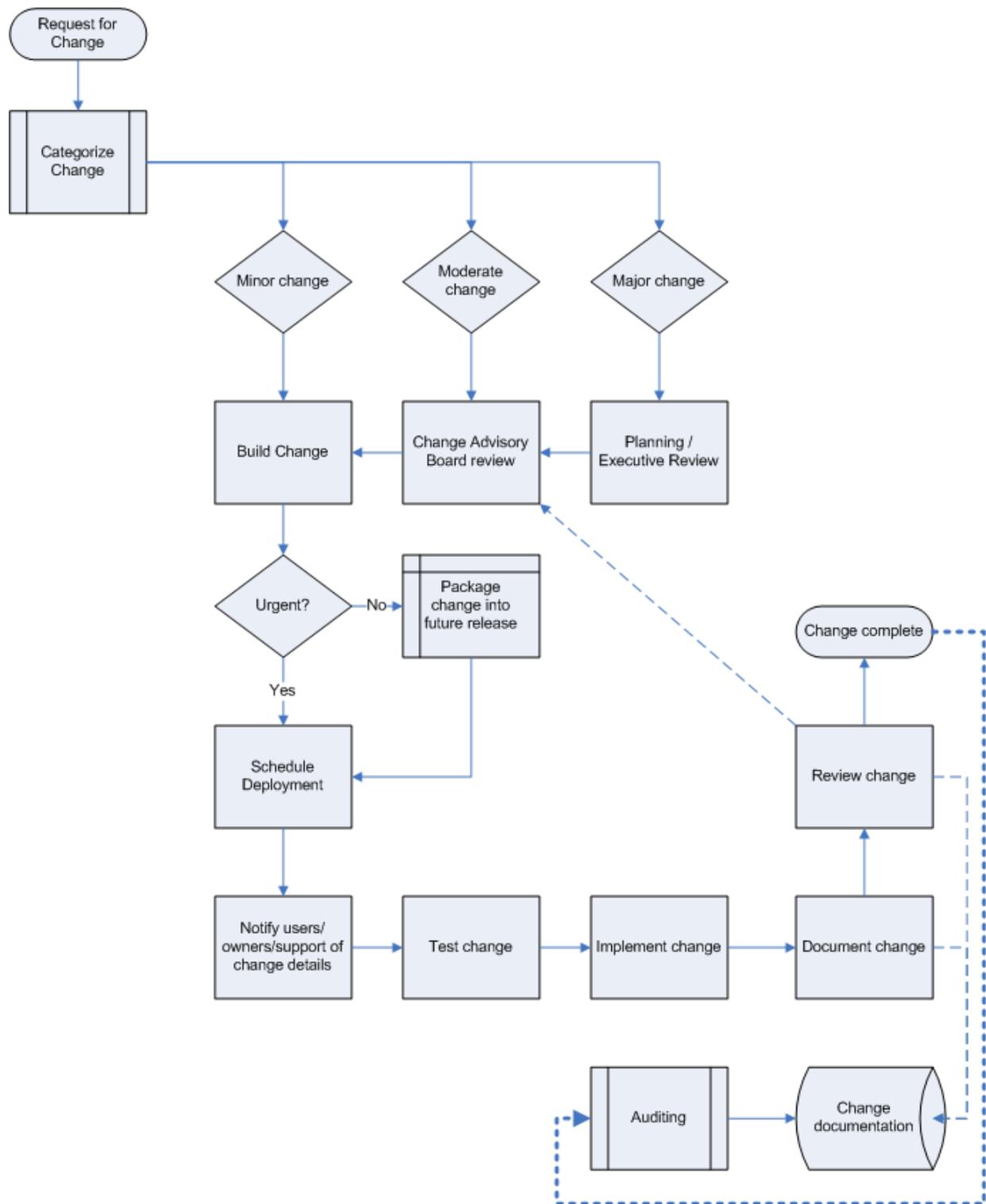


Figure 7.1: A simplified illustration of the ITIL change management process.

This process includes several discrete functional areas, including:

- **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).

 Later in this chapter, we'll explore in more detail who should make up the CAB and EC.

- **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.

In the next several sections, I'll discuss each of these activities in more detail.

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.
- **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 must 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.

Change Logging and Filtering

The purpose of change logging and filtering is to apply some sensible precautions to incoming RFCs. Primary goals include categorizing RFCs and allocating resources to handle them. ITIL recognizes that most companies have sufficiently complex bureaucracies already, and suggests several steps, including review time limits, designed to prevent change management from becoming an all-encompassing process that never actually gets anything done. “Shipping is a feature” is a common internal quote heard at many software companies. This thinking makes it clear that all the features in the world are useless if they’re not in users’ hands. ITIL adopts a similar attitude regarding change—change that is never implemented isn’t change at all.

Changes—or, more specifically, RFCs—occur for several reasons:

- To resolve a problem or incident, such as failed equipment.
- To resolve user dissatisfaction, such as an application that doesn’t offer necessary features or that provides an awkward user interface.
- To introduce new software, equipment, or other CIs into the environment.
- To upgrade an existing CI, such as a service pack for a software application or a firmware upgrade for a network device.
- To support a new or changed business direction, such as the need to connect to a business partner’s network.
- To comply with new or changed legislation, such as the security mandates that are becoming increasingly common in several industries.
- To become more competitive, such as adding a new section to the company Web site to accept online orders.

Obviously, some of these reasons—such as RFCs intended to address an immediate failure—are more urgent than others, and some—such as a connection to a partner network—require significantly more planning than others. The first phase of the change-management process, then, is assessing and allocating changes so that they are handled with appropriate urgency and in the appropriate order. Some RFCs might be rejected as being unsuitable, undesirable, or for other reasons; your process should incorporate an RFC appeals process to upper management for rejected RFCs.

Individuals submitting RFCs should be asked to classify their urgency. Although this classification might not be the final determination of the RFC's treatment, it provides input for the requestor's assessment of the RFC. Suggested urgency levels include:

- **Right Now**—Used for urgent changes without which a loss of service or functionality to many users has or will occur. The CAB or EC should give immediate attention to RFCs of this urgency. An example might be a router that is no longer functional.
- **As Soon As Possible**—No users are currently affected in such a way that they can't compensate, but a major loss of service or functionality is pending. The entire CAB should review these RFCs as their first priority. A branch office that is functioning on a backup network device is an example of this change level—especially if the backup device cannot handle the load of the original device.
- **Required Soon**—Although a loss of service is possible, there is no immediate or severe impact. However, corrective action cannot wait until the next scheduled release of changes, and so the RFC should receive medium priority at the next CAB review. An example is a patch to a router's OS when that patch resolves an issue that creates periodic, but very brief outages.
- **Next Release**—No immediate or severe impact, and the change can wait until the next scheduled release of changes. This item is low priority for the next CAB review. An example is a redistribution of users across network segments to improve network load balancing.

The CAB or EC needs to either actively agree with the RFC's original priority or modify it appropriately. RFCs that are downgraded in priority are not reviewed further, but are postponed until the appropriate, scheduled occasion for reviewing updates of the new priority level.

When the time comes for a CAB or EC assessment of the RFC, the following factors should be considered:

- How will this change affect the overall IT infrastructure?
- Will the change itself require maintenance downtime that might affect users or customers?
- Does the environment have the capacity for the change?
- How will the change affect disaster recovery plans?
- Will the change have an impact—positive or negative—on the performance of any aspect of the IT infrastructure?
- What is the potential effect of not implementing the change?
- What potential savings are gained by implementing the change?
- What potential costs might be incurred by implementing the change?
- What resources are required for the change (specifically, what personnel will be required? How much time will be needed? Will any new infrastructure be required?)?

I strongly recommend that these criteria be made available to individuals who might submit an RFC, and that they be encouraged to try and answer these questions within the RFC itself. Obviously, an emergency call in the middle of the day reporting a failed firewall isn't going to be written up in an RFC; the change request—to change the firewall's condition from “broken” to “operating”—might take the form of a Help desk trouble ticket and might not go through any kind of formal review process. That's normal, and will nearly always be the case for these reactionary situations.

However, for proactive situations in which the change is not mitigating or correcting some immediate negative condition, a review is a good idea. It lets you place the change into the context of your overall network. Sure, changing a routing table is an easy task, quickly accomplished by any administrator; but the impact on the environment can be significant and the actual benefit of the change might be negligible. The review process might, therefore, prioritize the change as Next Release, lumping it in with another set of changes in a more planned, orderly fashion.

Of course, this entire phase of the process depends heavily on RFCs that contain adequate information for the CAB and EC to make decisions. In some organizations, you might want to assign the task of creating RFCs to your Help desk staff or another organization, allowing them to assist end users and other non-technical personnel with the process of understanding and completing the RFC. To summarize, the information you'll need to collect in each RFC includes:

- The name of the requestor.
- The names and/or descriptions of the CIs being changed.
- Any proposed details on the change that are available.
- The business need or reason behind the change.
- A short summary of the benefit offered by the change.
- A short summary, if available, of the costs or downtime that the change will require.



Most non-technical individuals will not be able to provide this information; it might simply come down to a hunch by the reviewing CAB or EC.

- The proposed priority for the change.

The reviewing CAB or EC will need to ensure that this information is relatively complete in order to make an assessment. That assessment should also include an assignment of the change's impact: Minor, Moderate, or Major. This impact assessment will affect the next step in the process.

Urgent Changes

The ITIL model provides an expedited path for urgent changes, allowing them to be immediately and quickly reviewed, built, scheduled, and implemented. ITIL offers the following recommendations for keeping urgent changes a smooth part of the overall change management process:

- Assess urgent changes primarily for production impact and resource requirements. Worry less about cost/benefit concerns.
- If the CAB is available to review urgent changes, use it. However, if convening the CAB is not practical, use the EC to review the change.
- CAB (and EC) members must have both business and technical knowledge to accurately and quickly assess an urgent changes' impact. If the CAB or EC has to refer to technical specialists that are not already a part of the CAB or EC, the process will be slowed and eventually be discarded as unwieldy.
- The CAB or EC should make the final determination of urgency. There might be times, for example, when an urgent condition is allowed to exist because the business impact of correcting it would be too great.
- Changes classified by the CAB or EC as non-urgent should be immediately deferred to the next regular review meeting of the CAB.
- Because urgent changes are expedited and more likely to create negative impact or contain an error, rollback plans should be in place. An automated change management solution can help provide this recovery plan for network devices by providing a means of restoring earlier, known-good configurations to changed devices.
- A communication plan must be in place for quickly informing support personnel of the pending urgent change. Email is generally effective for this purpose.

Ensure that urgent changes are reviewed by the CAB at their next regular meeting to assess the successfulness (or lack thereof) of the change. Whenever possible, changes that negatively impact SLAs should be avoided.

Once changes have been assessed, they can be allocated and worked on. Changes that are considered very minor can generally be built and deployed directly by an administrator who has been delegated that authority by the change manager. For example, a regular change to a device's SNMP community string might be considered a minor change because it has a very low probability of causing negative end-user impact. Even if done incorrectly, it will impact only management operations and can be easily corrected or rolled back, if necessary. Regardless, the results of these changes should be documented and reported back to the CAB for future analysis.

More serious changes—that is, changes that have a broader potential impact, a longer build time, or affect a larger number of devices—should be reviewed by the CAB prior to implementation. Doing so will help ensure that the change is prioritized correctly and that disaster recovery plans are in place to recover from an error.

Changes with a major impact should be first reviewed by upper management, then passed to the CAB for scheduling and implementation. Such changes include sweeping infrastructure changes, long-term implementation projects, and so forth. Figure 7.2 illustrates the categorization portion of the simplified ITIL process.

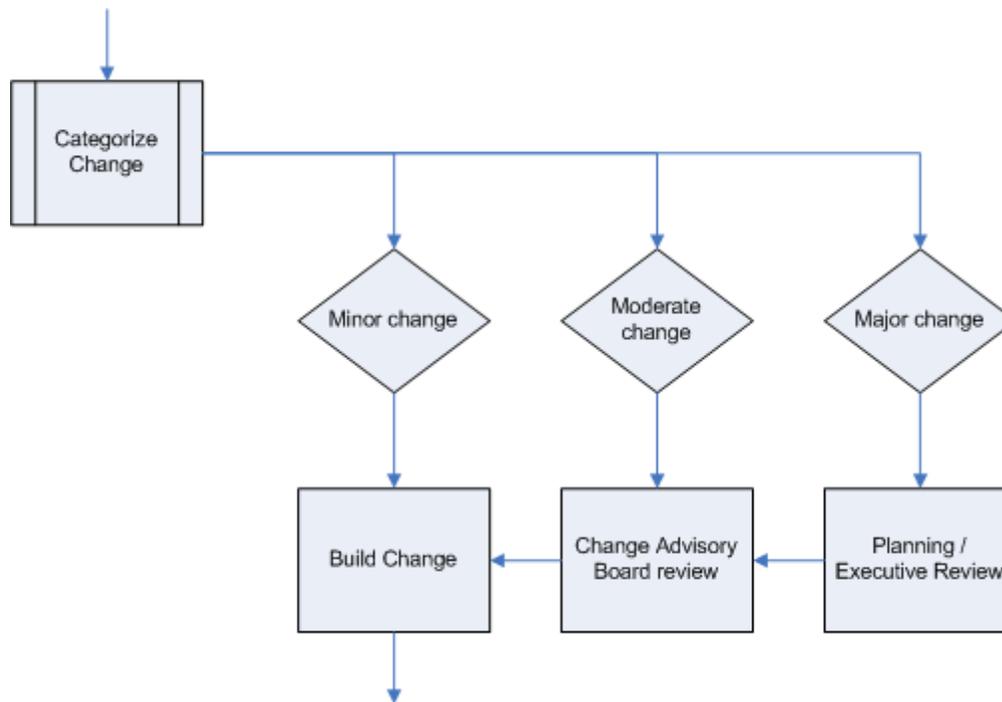


Figure 7.2: Categorizing change impact.

Reducing Bureaucracy

The ITIL recognizes that the formal creation of a CAB and EC, implementation of a formal change-management process, and introduction of the other management-related layers of the process can quickly create an undesirable bureaucratic layer in your organization. ITIL therefore provides recommendations for keeping the process a common-sense effort:

- Allow all IT staff to submit RFCs (rather than end users). The staff should act as a first filter layer for end users' requests, helping put RFCs into a usable form and ensuring that completely trivial requests are marked as low priority.
- The CAB should meet every 20 days for no more than 2 hours maximum, or in some other limited, predictable fashion. These regular meetings will set expectations for users who submit RFCs to the IT department. The EC is available as an expedited review entity for urgent changes.
- If you're moving from another change-management process to a more ITIL-compliant one, cut over immediately—don't run parallel processes, which will simply act to gum up the works.
- Implement a defined period for reviewing changes (for example, 30 days after completion). This defined period ensures that all changes are reviewed at the proper time.
- Require contractors working within your environment to comply with your change-management process. Allow absolutely no changes to occur outside the process.

As I pointed out earlier, acknowledging that the purpose of change management is to *facilitate* change—rather than make it an exercise in paperwork and meetings—will help keep the process trim and usable. If you find that your CAB is spending more than a couple of hours a month reviewing changes, you need to seriously examine the nature of those changes; perhaps it's possible to roll them into a larger, more comprehensive project that can be treated as a single major change to the infrastructure.

Managing Changes and the Change Process

Once reviewed by the CAB, the change is considered accepted (unless, of course, the CAB rejects it) and enters the more straightforward, implementation portion of the change-

management process. Figure 7.3 illustrates this portion of the process, which includes scheduling, building, and implementing the change.

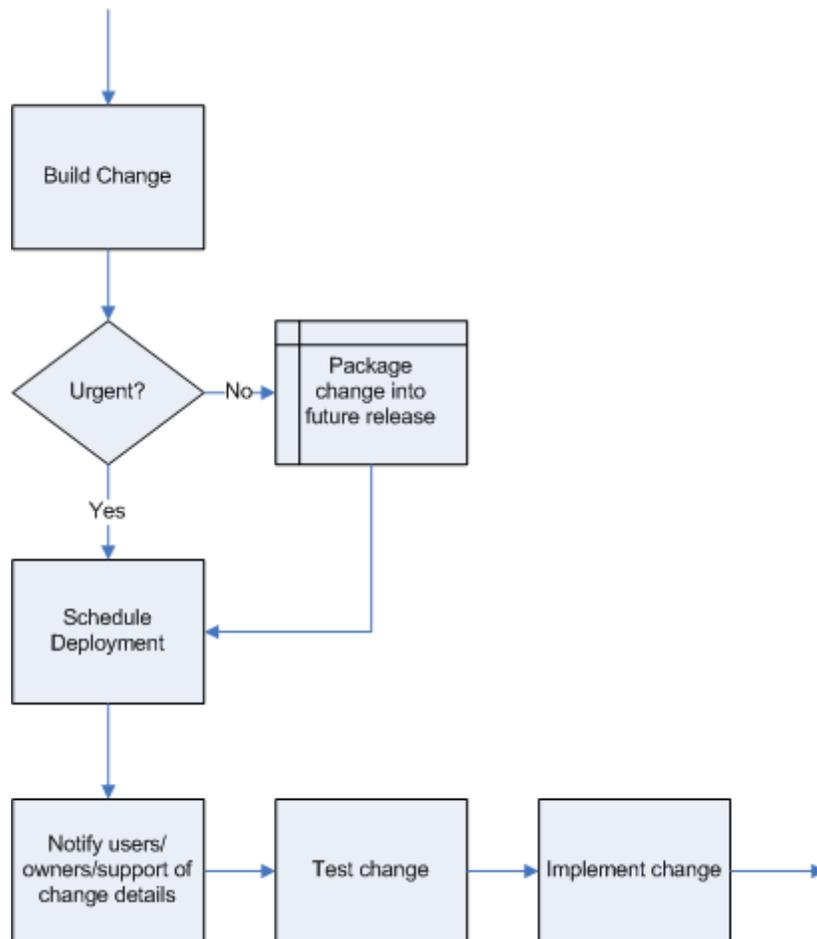


Figure 7.3: Scheduling, building, and implementing the change.

Whenever possible, changes should be packaged together into *releases*. A release is simply a group of changes (or introductions of new CIs) into the environment. The IT industry has a sort of general distaste for releases, often feeling that making too many changes at once is asking for problems. This feeling comes from times when IT professionals have introduced a series of changes, only to have all of them go wrong—meaning they’re now swamped in mitigation activities. After that horrible experience, they introduce changes slowly—one at a time—and fix problems as they come up.

Had the changes been properly planned and reviewed in advance, they would have been much less likely to cause problems. Packaging them together into a bundled release would have represented *one* opportunity to simple human error to cause a problem. Another way to look at it: Every time you open something for changes, you might click a wrong button or take some other unintended action and cause a problem. Bundling changes into a release provides few opportunities for ancillary complications. A configuration management tool that helps deploy changes can also reduce error by consistently applying changes to multiple devices with much less possibility of wrong buttons being clicked or incorrect commands being entered.

However, release size should be managed to a reasonable standard. Introducing 300 new changes in a single morning might, for example, be beyond the capability of your support organization. It's a proven fact that Help desks are often swamped with calls after changes are made to any visible portion of the IT infrastructure: Users distrust change and often become confused when confronted with new processes and procedures. Thus, intelligently packaging your releases into a manageable size will help keep any subsequent, non error-related support issues at a manageable volume.

The CAB and EC play an important role in scheduling. Lower-priority RFCs might get bumped to later and later releases in order to make room for higher-priority releases, while keeping the size of the overall release at a manageable size. The CAB must maintain the balance between the business' needs and the technical issues resulting from changes. All such decisions should be documented, providing subsequent CAB reviews of each RFC with some context of why the RFC is where it is in the process. Figure 7.4 shows a sample release schedule, visually depicting RFCs that have been bumped to later releases.

Release 701 – August 2004

RFC	Desc	Priority	Impact
14231	New router	2	Moderate
14232	Router IOS flash	2	Moderate
14233	Switch IOS flash	2	Moderate
14235	New firewall config	1	Major

Release 702 – September 2004

RFC	Desc	Priority	Impact
14234	Change perms	3	Moderate
14236	Upg 2 switches	2	Moderate
14239	New segment	2	Major
14240	New router card	3	Major

Release 703 – October 2004

RFC	Desc	Priority	Impact
14238	Fix serial interface	4	Minor
14237	Flash VPN IOS	3	Moderate
14241	Upg RIP, 2 rtrs	2	Moderate

Figure 7.4: Graphical release schedule showing delayed RFCs.

Change production is one area in which ITIL falls short in terms of best practices. ITIL suggests that authorized changes be passed to technical personnel, who actually develop the change. In the case of network devices, that usually entails building a new configuration file for a device, specifying new hardware, or something similar. Rollback procedures (called *back-out* procedures in most ITIL documents) must be documented at the same time; an automated network device configuration management solution can often provide built-in configuration rollback capabilities in the case of device configuration changes. However, for more hardware-level changes, such as implementing a new network segment, be sure some physical rollback plan is in place.

ITIL also suggests that the change be tested, which is of course a good idea. ITIL's idea of testing, however, is to more or less maintain a mirror of the production environment for testing. This suggestion is completely reasonable in the case of software applications—which is, in fact, where most of ITIL's change management process comes from—but wholly impractical in the case of physical network devices.

ITIL also neglects a formal peer review process. In the absence of practical testing in a mirrored test environment, peer review is absolutely essential to help ensure that changes don't contain errors or create unexpected conditions. Figure 7.5 shows an illustration of a modified simplified ITIL process that incorporates an iterative peer review process—something I've discussed at length in previous chapters—in place of the ITIL testing step.

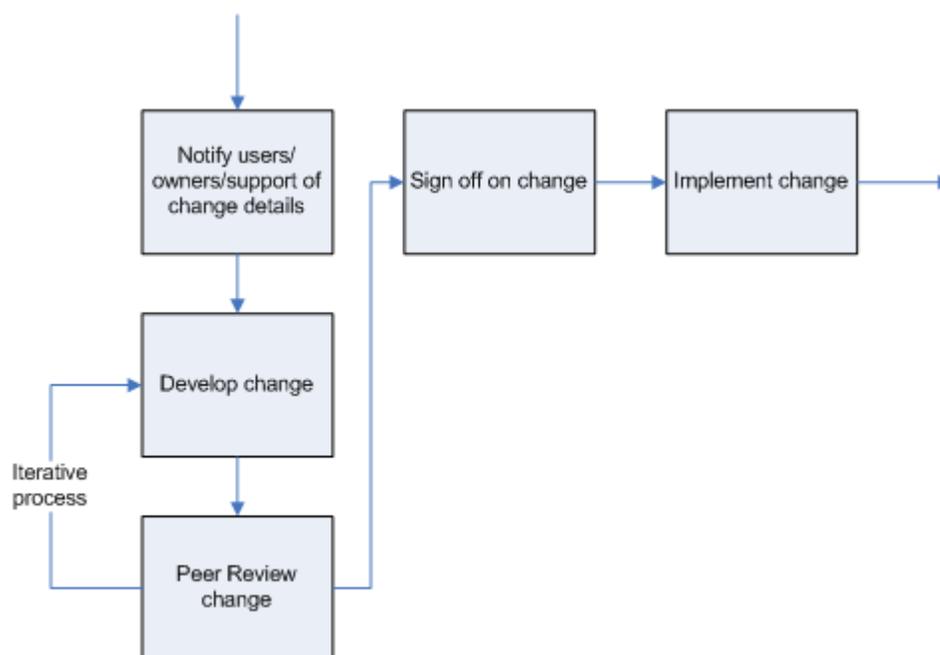


Figure 7.5: Incorporating a peer review into the process.

Keep in mind that an effective network device configuration management solution can help facilitate peer review by making proposed configuration file changes available to the reviewer and incorporating a workflow process that helps ensure that all changes are reviewed and approved before being deployed by the solution.

Finally, with the change built and approved, it is ready to be deployed. The change manager's job is to ensure that changes are deployed on schedule and that the change is deployed successfully. The change manager should also ensure that communication channels exist to inform support personnel of exactly when a change will occur and to confirm that it has been implemented in the production environment.

In the case of network devices, because full-scale testing isn't often practical, that the CAB or EC should make a recommendation for the change's deployment timeframe. Changes considered moderate or major in impact might only be deployed during off-peak hours, ensuring minimal production impact in the event of a problem. Minor changes or those of an urgent nature might be cleared for deployment during regular working hours or during peak network usage.

I can't stress enough the important role that constant communication plays in the overall process. I've been in a number of environments in which lower-tier support personnel took corrective actions with the belief that an announced change had already been implemented, when in fact it had been delayed. Communications need to occur whenever:

- A change is announced
- A change is scheduled for deployment
- A change is successfully deployed
- A change's deployment is delayed or cancelled
- A change is rolled back

 If you use email to make these announcements, send them all from a single email address or alias. Doing so will allow technical support personnel to implement local rules on their email client to specially color-change announcements or highlight them in some other way so that the messages stand apart from the usual flow of email in the business. Encourage personnel to implement these rules so that important change-related announcements aren't "lost in the shuffle."

The CAB

The makeup of your CAB (and its subset EC) is extremely important. First, understand that the CAB is intended to be a somewhat dynamic organization: If you're reviewing changes related to the network infrastructure, the CAB should be comprised of people who understand the business and technical issues of that infrastructure.

Because the ITIL change-management process is intended to address all aspects of change—including software, servers, client computers, infrastructure, and more—ITIL assumes that a separate CAB will exist for each (although each CAB might have overlapping members, of course).

The CAB should be small. The change manager, one or two business-savvy members, and a couple of senior technical professionals should be sufficient. The goal of the CAB is to meet, quickly review pending RFCs—remember, just a couple of hours every 2 to 3 weeks should be sufficient—and move on. A large CAB will almost invariably result in too much "management by committee," which will simply defeat the change-management process and result in a motionless bureaucracy.

Coordinating Change

In the ITIL framework, coordinating change is the responsibility of the change manager in your organization. Coordinating change is one part change management and one part project management, as Figure 7.6 shows.

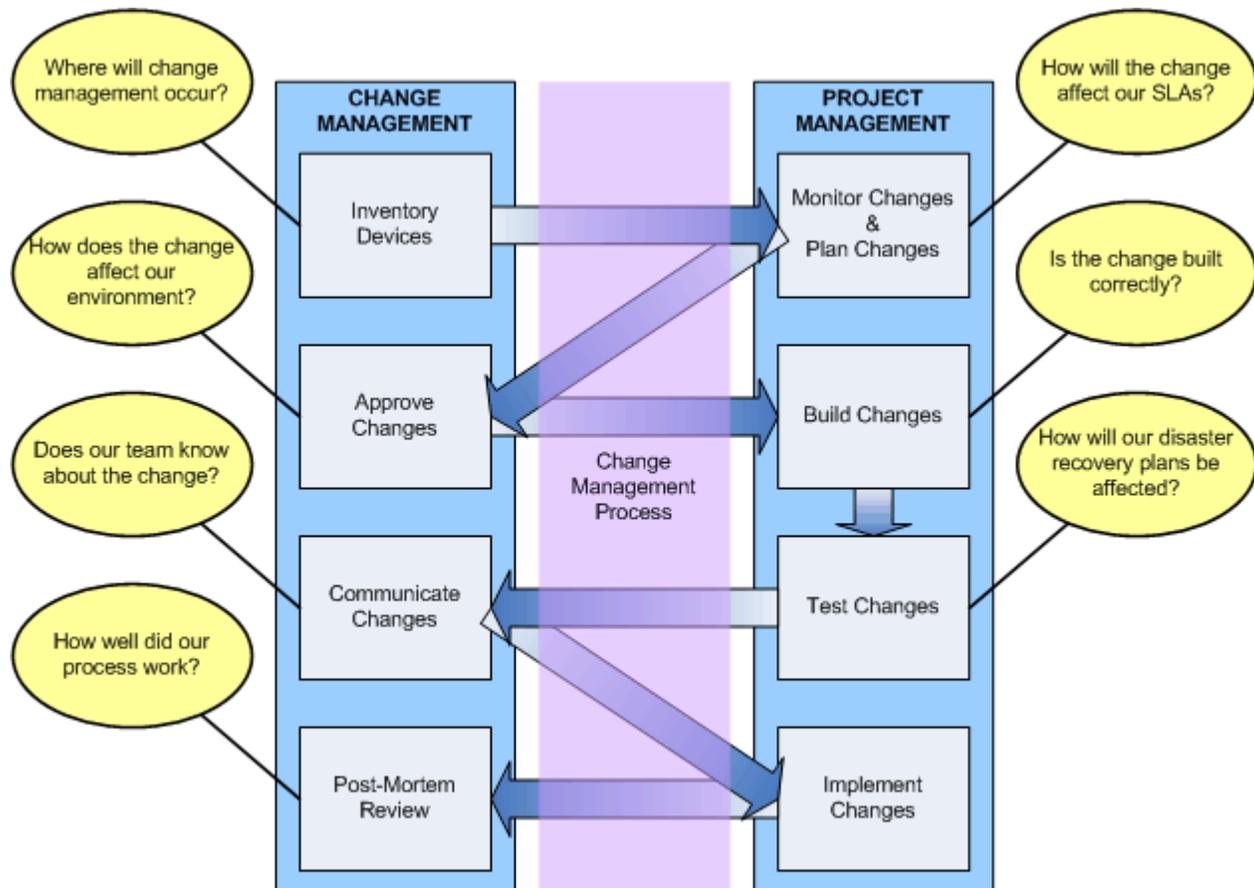


Figure 7.6: Change and project management work together.

The basic change management process consists of four tasks that involve actual change management:

- Inventorying CIs (network devices, for example)
- Approving changes
- Communicating pending changes
- Reviewing completed changes

These are the primary responsibilities of the change manager. Other management steps occur, but are more technical in nature and classified as project management:

- Monitoring CIs for changes and planning new changes
- Building changes for deployment
- Testing changes and updating contingency plans
- Implementing changes

Although these tasks will often be undertaken by someone other than the change manager, Figure 7.6 shows that the interaction between change and project management is frequent. The individuals managing these two activities need to communicate constantly to ensure the proper flow of the overall change-management process.

Reviewing and Closing Requests for Change

The last step in the change-management process is a post-mortem, or final review of how the change implementation went and how well the process worked. You should consider a number of criteria in your post-mortem:

- Are end users satisfied with the results of the change? In the world of network device management, users being completely unaware of the change constitute satisfaction.
- Were there any unexpected side effects from the change? If so, did they interrupt operations or require additional changes to correct or mitigate?
- Can the change be left in place? Changes that are rolled back are considered unsuccessful, because you can assume they will need to be rebuilt, retested, and redeployed at some future time.
- Were the resources used to implement the change the ones that were planned? Were additional or fewer resources required? This review point is important for helping the CAB and EC refine future resource estimates.
- What did you learn from this change that can be applied to future changes, especially ones that are already in the queue for implementation? This step is the perfect time to apply “lessons learned” to upcoming scheduled changes and prevent a repeat of any problems that occurred this time.

A basic report should be made available to the CAB or EC, and in the case of more major changes, to upper IT management. This report should summarize the original goals of the change, detail how the implementation occurred, and list any problems along with, if possible, their reasons.

 Listing the reasons for an unsuccessful change shouldn't come down to finger-pointing. Reporting that “John messed up the BIOS flash” isn't helpful unless you're trying to fire John; reporting that, “Administrator error caused the wrong BIOS image to be downloaded” is useful information. You might use that information in future changes to, for example, have a peer verify that the correct BIOS image has been selected prior to downloading.

Auditing and Management Reporting

Auditing and reporting is an important part of the change-management process in ITIL. Management reporting is essential to measure the effectiveness of the change-management process. Some overall goals of this process include:

- A reduction in the number of negative impacts that changes to the IT environment have on end users and other business processes.
- A reduction in the number of problems associated with changes.
- A reduction in the number of changes that must be rolled back.
- A reduction in the number of unplanned, urgent changes.
- An improvement in change invisibility. In other words, changes shouldn't be readily noticeable outside the change-management process itself.
- All actual changes should flow through the change-management process.
- High-priority RFCs should not be backlogged, and the backlog of changes should either shrink or remain relatively constant in size.
- The process of estimating the resources required to implement a change should become more accurate.
- RFCs are reviewed regularly, and changes are reviewed promptly and regularly after being made.
- The number of rejected RFCs should diminish—if such doesn't occur, further education about the role of change and the change-management process is necessary.

Auditing plays an important role in ensuring that the process works effectively. Auditing is a chance to objectively review everything about the process, including changes that might have occurred outside the process. Auditing can provide a frank view of the process' failure and successes, and an opportunity to revise and refine the process for continual improvement.

Auditing should focus on randomly selected RFCs, formal records of changes, minutes from CAB and EC meetings, change implementation schedules, and the records and reports associated with closed and completed RFCs. The goal of auditing should simply be to highlight areas in which the formal change-management process wasn't followed, allowing the change manager to put more focus on maintaining the integrity of the process.

Change Management Challenges

ITIL recognizes that change management won't be universally accepted or successful, at least not at first. Auditing plays a role in keeping things on track, but understanding *why* change management can fail as a process can help you prevent problems. Common reasons include:

- Record keeping—Paper-based record keeping systems are doomed to failure in all but the smallest IT shops. In the previous chapter, I introduced you to several categories of tools that can aid in electronic record keeping and process automation; use them.
- Culture—Organizations that have maintained a more casual attitude regarding IT might face considerable personal and cultural challenges: Administrators might feel that the process is designed to micromanage them, for example. Education is the key to overcoming this obstacle. Be prepared to show how unmanaged change has resulted in unnecessary downtime, repeated work, on-the-job stress, and more.
- External-process change—Change made outside the change-management process not only carries the risk associated with all unmanaged change but also impacts managed changes that are proceeding without knowledge of the unmanaged changes. Fortunately, automated network configuration management tools can be configured to automatically detect most unmanaged change, alerting you to it and allowing you to take appropriate corrective action.

Be sure you plan for these and any other challenges in your environment. Solicit feedback from users, managers, and administrators to find out where your obstacles will be, and start preparing to work through them.

ITIL Configuration Management

In the ITIL world, *configuration management* is somewhat more analogous to *asset management*. Its goal is to control CIs (such as network devices), continuously confirm their status, and audit them to ensure that they remain configured properly. There are actually four primary steps to the ITIL configuration management process:

- Identification
- Control
- Status
- Verification

Because ITIL configuration management is really a form of asset management, I'm going to cover it only briefly. The ITIL change-management process really focuses on the internal software configuration of network devices and is the most appropriate model to use when developing a process to manage those devices. Configuration management (ITIL-style) certainly plays a role, but it's a much less complex process.

Identification

This step requires to you positively identify each asset, or CI, under your control. On small networks, this task is easy; on larger networks, you might want to use an automated network configuration management tool to help identify and inventory resources for you.

Your inventory should be comprehensive and include device type, name, model, revision or build level, installed options (such as memory, expansion cards, and so forth), serial number, and so on. Ideally, your inventory should be detailed enough that a non-technical individual could acquire an exact replacement unit should the need arise.

Control

The goal in this step is to ensure that CIs are not altered or replaced without authorization. That authorization should come through your change-management process, which I described earlier in this chapter. Ideally, you should implement an automated solution, such as a network configuration management solution, that can inform you of unauthorized changes to CIs.

Status

You need a means to continually confirm the status of your network devices. Automated tools can help with this step, verifying that CIs haven't changed since the inventory or last approved change.

Verification

Auditing should be a manual process that matches physical devices to your inventory and change schedule. This step ensures that the process is being observed and that your on-hand assets match your configuration management database.

Assessing Your Practices

As I mentioned earlier, there are several consulting companies who will be happy to assess your current configuration and change-management practices to help you direct them more toward the ITIL standard. None of these represent any kind of formal process certification along the lines of ISO9001, but they can still be useful. You can also purchase self-assessment packages, which usually cost about \$200 and include several spreadsheets that walk you through a sort of interview in which you rate various aspects of your current processes. The product then scores you for ITIL compliance and offers pointers for improving your processes by using the ITIL standards.

To get you started on a manual assessment, I'll walk you through a brief assessment that I've used with consulting clients in the past. This overview isn't intended to be a complete ITIL assessment (it focuses mainly on change management, not the entire IT services discipline), but it will hopefully help you highlight areas of your change-management process that need focus for improvement or formalization.

Assessing Your Change Filtering Process

Ask yourself the following questions. For each “yes” answer, give yourself one point; for each “no” answer, give yourself zero points:

- Do you have a formal process for submitting change requests?
- Does someone review change requests and assign them a priority?
- Are change requests reviewed by a small panel that spends no more than 2 hours each month (approximately) reviewing changes?
- Are change requests reviewed by individuals who have both a business and technical insight into the changes and their impact?
- Is there a process for rejecting change requests and a process for requestors to appeal the rejection?
- Are changes assigned an impact level and reviewed, as appropriate, by upper levels of management?
- Are lower-impact changes expedited and cleared for implementation without excessive review?
- Does a smaller review panel exist for urgent changes to be reviewed?

Assessing Your Change Implementation Process

Ask yourself the following questions. For each “yes” answer, give yourself two points; for each “no” answer, give yourself zero points.

- Are disaster recovery plans reviewed and revised, as appropriate, each time a change is made?
- Are changes tested or peer reviewed prior to implementation?
- Is a mechanism in place for detecting out-of-process changes and notifying an administrator of them?
- Are changes scheduled for packaged releases when possible?
- Are urgent changes moved through the process more quickly?
- Are changes scheduled for implementation based upon their production environment impact?
- Do almost all (95%) changes pass through the change-management process prior to implementation?

Assessing Your Change Review Process

Ask yourself the following questions. For each “yes” answer, give yourself one point; for each “no” answer, give yourself zero points.

- Are changes reviewed after completion for accuracy?
- Is the change-management process reviewed for compliance and completeness?
- Are errors and mistakes documented and used to modify upcoming changes or the overall process?
- Is an auditing plan in place to randomly audit various aspects of the process for compliance?

Scoring Your Results

How did you do? If you scored less than four points for your change filtering process, you probably need a more solid, ITIL-style process for accepting, filtering, and categorizing change. Implementing such a process is the first step to a change-management process, because the change filtering step is what filters all input to that process. As the old saying goes “garbage in, garbage out;” without filtering the input to your change-management process, you can’t expect it to succeed.

If you scored less than 10 points in the change implementation category, you probably don’t have a formal change-management process in place, or your process is incomplete, not enforced, or poorly defined. Using the examples in this guide to define a formal change-management process and ensuring that all changes are passed through that process will help you achieve the benefits of greater uptime, greater security, greater stability, and reduced cost and effort.

If you scored less than three points in the review category, you’re not devoting sufficient time toward ensuring that your process works, ensuring that your process is followed, and applying lessons to future effort. Without an adequate review and audit process, your entire change-management process might as well not exist.

The maximum overall score was 25. If you scored less than 20, you probably don’t have a robust change-management process. If you scored less than 15, the process you do have, if any, is probably incomplete enough as to be a waste of your time. A score of less than 10 indicates that absolutely no formal process is in place or that the process in place isn’t followed consistently or applied for best effect.

Summary

The IT industry is a challenging, always-changing one, which makes it difficult to develop best practices. Authors can preach good ideas based on long experience and lessons learned, but it's easy to disregard such advice as coming from one source without experience in your particular environment. ITIL, however, is the result of years of experience by hundreds of practitioners in a variety of industries and organizations. It's a formal set of best practices, documented and detailed, and applicable to almost any IT effort. This chapter has provided you with an overview of ITIL's change and configuration management best practices as they apply to network device configuration management; hopefully you'll be able to use this information as a formal starting point for your own change and configuration management processes.

In the next chapter, I'll finish this guide by going over several sample processes that you might adopt. These will be based on large part on the previous chapters of this book and the ITIL best practices, with each process tweaked to meet slightly different working conditions.