Strengthen your own compliance program

Make IT compliance easier

Your first IT compliance experience was probably challenging. So, you're probably looking for an easier way to pass future audits. Look no further. With *IT Compliance For Dummies,* Limited Edition, you find out everything you need to know about developing a sustainable IT compliance program that reduces compliance risk and resources. With this book, you get information that helps make IT audits easier while avoiding common pitfalls.

THE DUMMIES WAY

- *Explanations in plain English*
- *"Get in, get out" information*
- *Icons and other navigational aids*
- *A dash of humor and fun*

ISBN 0-471-75280-0

Discover how to:

- *Create a sustainable IT compliance program*
- *Make the next audit easier*
- *Derive a strategic advantage from your efforts*
- *Tackle common IT control gaps*

Get smart! @www.dummies.com

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Sign up for eTips at etips.dummies.com*

For Dummies®
A Branded Imprint of
WILEY

Reduce compliance risk and resources

IT Compliance FOR DUMMIES®

Limited Edition

Simplify and control your next IT audit

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Clark Scheffy
Randy Brasche
David Greene

IT Compliance FOR DUMMIES® LIMITED EDITION

by Clark Scheffy, Randy Brasche, and David Greene

Wiley Publishing, Inc.

IT Compliance For Dummies®, Limited Edition

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN-13: 978-0-471-75280-6

ISBN-10: 0-471-75280-0

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1S/QW/QZ/QV/IN

Table of Contents

Introduction

Compliance is all about doing what you said you were going to do. Sounds easy enough, right?

Although every company and IT organization has internal compliance (policies, procedures, rules, guidelines, and so on), every company approaches and enforces compliance differently. Some do so more consistently than others.

Because of recent Sarbanes-Oxley requirements, compliance is more important than ever. In fact, your organization has probably already survived its first audit. Probably, you found the first round of Sarbanes-Oxley compliance challenging to say the least. You are not alone. Most companies found the first round of Sarbanes-Oxley compliance to be time-consuming, confusing, and expensive.

So how can you make the next audit easier? That's where this book comes in. We show you how to develop and create a sustainable IT compliance program that tackles the major IT control gaps identified by auditors. We also show you how you can derive a strategic advantage from your compliance efforts.

Assumptions

The chapters in this book all present a different component of the compliance equation to help you develop your own sustainable compliance strategy amid ever-evolving Sarbanes-Oxley compliance requirements.

We are writing this book with the assumption that you are past your first audit and in the process of planning for future audits. We guess you are an IT professional. We also hope you will pass this book around to your colleagues and that doing so will start important discussions for how you will handle your compliance needs.

How This Book Is Organized

This book is organized into two parts. Part I, with five chapters, starts with some compliance basics in Chapter 1. Chapters 2 through 5 each cover a different element of a sound, sustainable compliance strategy.

Part II is the Part of Tens, containing two chapters. The first chapter shows you ten ways to leverage your compliance effort as an opportunity. The second is a quick list of the ten most useful things to remember when putting in place an ongoing, sustainable compliance strategy.

Icons Used in This Book

Some information we present in this book warrants highlighting for extra attention. We identify this material with one of the following icons.

This icon identifies, not surprisingly, a tip — some piece of information that will make things easier or help you avoid a common pitfall.

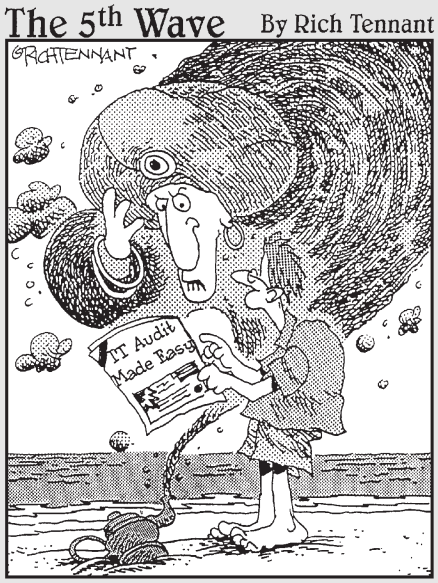
This icon highlights something that may cause trouble if you don't use due care.

When you see this icon, we are digressing into some details that are not absolutely essential, but which may be interesting nonetheless.

If you see this icon, the accompanying text will be invaluable as you go forward.

Part I

Developing Your Compliance Strategy



"Can't I just give you riches or something?"

In this part . . .

This part starts with a chapter on the basics of compliance — how we got here, where we are going, and what you have to do about it. The rest of the part includes chapters that address the major components of a sound, sustainable compliance effort.

Chapter 1

Learning from Your First IT Audit

In This Chapter

- Understanding how we got here
- Identifying the major challenges to compliance
- Avoiding being wagged by your auditor
- Achieving a strategic advantage through compliance

Compliance isn't new. A variety of compliance requirements from *HIPAA* (Health Insurance Portability and Accountability Act), *GLBA* (Gramm-Leach-Bliley Act), and *Basel II* (Basel Committee on Banking Supervision) exists for specific businesses. Pharmaceutical companies have long been highly regulated and must comply with strict compliance regulations.

With the advent of Sarbanes-Oxley legislation (SOX), compliance has taken the spotlight for *all* publicly traded companies. SOX has caused every publicly traded company in the United States to struggle to understand what it means to become "compliant." And because IT processes are critical to maintaining the integrity of a company's financial applications and systems, compliance is now woven into the fabric of the IT organization.

Unfortunately, most companies weren't fully prepared for "IT" during the first round of SOX. In fact, a recent survey found that 94 percent of executives attributed the company's compliance deficiencies to IT. Figure 1-1 shows this and some other interesting statistics.

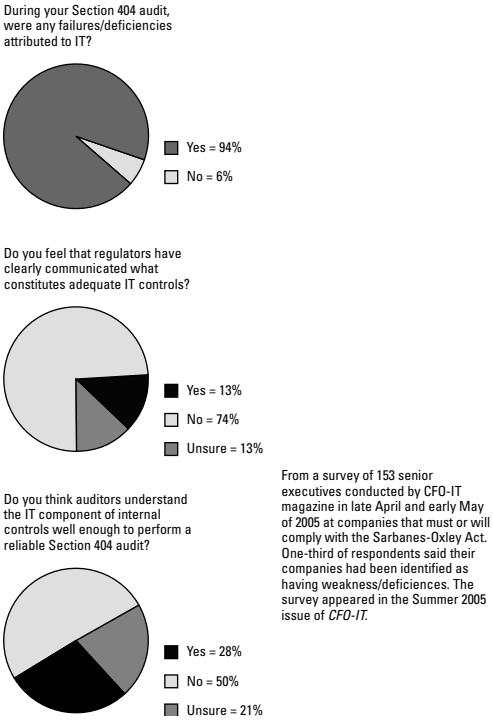


Figure 1-1: How do executives feel about the role of IT in SOX compliance?

Planning Ahead

Now that the horrendous first year is behind you, you have the opportunity to manage ongoing compliance and avoid the reactive "firefighting" response.

Companies and IT organizations are required to continually demonstrate compliance and most can expect even more work ahead of them. First, companies need to fix the deficiencies and gaps identified from last year. Next, they have to prepare to pass this year's audit. Finally, companies are struggling to catch up with all of the day-to-day IT work that was put on the back burner as a result of last year's audit. Now is the time to plan a long-term strategy so that you can manage compliance — not let it manage you.

The Big Challenges

Achieving IT compliance this year, next year, and every year in the future means addressing the fundamental challenges encountered during the first audit.

Identifying, documenting, and evaluating controls

Scoping and identifying your IT controls was probably the most challenging and frustrating part of your first compliance experience.

In the absence of proper guidelines and for fear of flunking an audit, many IT organizations created *way* too many controls. Better to be safe than sorry, right? As companies prepare for their next audit, they are facing a new problem: How do you manage and retest the excess of controls created during the first audit?

Your auditor may request more controls than are necessary. Be sure to discuss questionable controls with your auditor so that you can minimize the volume of controls that require testing and management. This discussion doesn't need to be antagonistic — fewer controls for you also means less work for your auditor.

When testing and evaluating your controls for the next round of audits, be specific and focus on those controls that would have an obvious impact on the financials. For example: Who has access to what information? Who has the ability to make changes to the systems and applications?

Evaluating operational effectiveness through testing

The IT controls you established during your first audit will need to be continually evaluated and verified. You need to know as soon as possible where the controls are working and where they aren't.

This evaluation process is most commonly referred to in today's compliance environment as *testing*.

As some companies found out the hard way, waiting until the external auditor arrived to conduct testing was too late. Waiting until the internal audit was also late. The key is to make testing part of your ongoing operations.

You will be required to retest your IT controls during the next set of internal audits. Afterwards, you get to

do it all over again for the external auditors. The more controls, the more testing that will be required.

Identifying and remedying deficiencies

During the first round of audits, auditors identified several common control gaps and deficiencies that existed in most IT organizations. Unless addressed during the next audit cycle, these deficiencies can become material weaknesses. Material weaknesses can bubble up to the final filing and have an effect on the financial results.

Most IT organizations are scrambling to address the deficiencies uncovered during the first audit. IT organizations don't want to be responsible for a material weakness in a company's financial filing. We discuss some of the common IT control gaps in Chapter 5.

The Big Solution

The rest of this book points you in the right direction to step up to these challenges and create a sustainable IT compliance program that tackles some of the trickiest IT control gaps identified by the auditors.

Creating a sustainable IT compliance program provides additional benefits for your IT organization through improved operations and increased application availability.

Compliance is *not* going away. Every year, your IT controls will evolve with changing requirements. And, the auditors will be back every year to evaluate your IT control effectiveness. So how do you stay in compliance and keep up to date without reinventing the wheel every

year? The answer is to implement tools and processes for a sustainable compliance solution.

Companies can leverage a variety of strategies to make compliance sustainable. Best practices point to four key areas:

- Automating the IT control testing process
- Closing the loop in the change management process
- Managing and minimizing the list of IT controls
- Tackling the most common IT control gaps

The upcoming chapters are devoted to addressing each of these areas in greater detail.

Chapter 2

Automating the Testing Process

In This Chapter

- Saving time and money with automation
- Selecting areas of your organization to automate
- Validating your IT controls
- Remedying gaps in the shortest possible timeframe

Ultimately, *compliance* is testing your controls and generating the appropriate reports to show that you "did what you said you were going to do." During the last audit, you most likely threw bodies at the IT compliance problem to test, validate, and audit your IT controls through a plethora of reports and documentation. This method of compliance costs a lot of money and takes your IT personnel off their primary IT tasks.

The solution to this situation is to build automation into your compliance framework. Through automation, your testing and reporting are streamlined and also more consistent and accurate (which makes your auditor happy as well).

The benefits of automation include

- Reduced resource load and less money spent
- Ability to reallocate your compliance resources back to the business of IT
- Increased reporting accuracy and repeatability
- Ability to test and report consistently across multi-site locations

The more manual controls used, the more questions the auditor will ask — and the more nervous he or she will be about your internal controls being consistently followed.

Manual Testing versus Automated Testing

Today, many IT organizations test their IT controls through an ad hoc process of verbal confirmation, spreadsheets, and e-mail. This method is unreliable, to say the least.

Many auditors now require IT organizations to test their controls from "system generated" reports (meaning automatically generated from the operating system or application) to obtain an accurate record of changes made to financial applications. Proper compliance should, and in the future likely *will*, *require* an automated data collection process.

System-generated reporting is

- More reliable than human/manually generated reports.
- Less expensive to gather and collate than human/manually generated reports.

If you can improve reliability and reduce cost through automated, system-generated testing, your audit will be less expensive and require fewer resources.

So, which areas should you consider for automation? The following section tells you what to look for.

Choosing the Best Candidates for Automation

Choosing the best candidates for automation is relatively simple — focus on the manual, time-intensive IT controls that require forensic data from systems and applications. For example, a control that is currently validated through interviews, having people fill out forms, or walking through the data center with a clipboard is not a good candidate for automation. But a control that is validated by logging on to servers, reviewing change requests, or sifting through security logs is a prime candidate. These activities can include auditing direct access to systems, database access, and change management controls, all of which are discussed more throughout this book.

PricewaterhouseCoopers estimates that only 20 percent of large companies have automated their IT controls. Automating now is an opportunity to get way ahead of the curve and impress your auditor.

Automating the Prime Candidates

For proper automated IT control testing for change management and direct access, your system needs to properly detect all relevant change activity from your IT systems supporting financial applications — automatically. For example, you may want to report all changes to servers associated with your financial systems. You then need to review these changes to determine whether the changes violate policies or represent a significant problem.

Seeing who's doing what

The most obvious way to think about automated IT control testing for change management and direct access is to inspect who's doing what.

Sometimes, it makes sense to collect a broad set of data that may relate to multiple controls. The following components of your IT system may be considered "material" in the parlance of your auditor, which is to say that they have potential direct bearing on the accuracy of your financial reporting.

- **Direct Access:** People logging on to sensitive financial servers or databases. For example, the intern with permission to access any server within the IT department is *bad*.

- **Database:** Changes made to databases housing financial data. That is, someone changing the sales figures for Q4 from $1M to $10M in the database is *bad*.
- **Files and Registry Keys:** Files or configuration settings supporting financial applications. Someone changing the backup configuration for all financial data is *bad*.
- **Active Directory and LDAP Systems:** User access permissions and modifications to financial systems. If the junior employee has super-user access to all systems, that's *bad*.

Reducing audit costs with automation

Consider the *return on investment* (ROI) for automated testing of your IT controls. Your auditing and testing costs can be broken down to three basic components:

- **Direct expense.** You have to pay your personnel for their time. Automated testing saves time, and often considerable overtime, that would have otherwise been spent creating, gathering, and aggregating reports for an upcoming audit.
- **Audit expense.** Automated testing saves the costly time of your auditor by providing consistent, accurate reports prior to and during your audit.
- **Cost of downtime.** Automated testing tells you what changed at the moment a system goes down. So, the time for problem resolution and recovery is drastically reduced.

What the auditor wants to know is whether these components were changed by the people who have the appropriate and approved permissions to alter them, or not.

You may also want to audit all activities that are specific to defined control points. You can then use this report to identify the behaviors violating your policies. For example, a compliance report may track all changes made to critical configuration files or source codes files for a financial application, when the changes were made, and who made them.

Reviewing the results

So, you've collected all of this data by detecting "who is doing what" to the infrastructure. Now, what do you do with it?

The next step in automation is to bring the collected data together in a tool or format that allows easy review. Depending on the control you are trying to validate, you need to "visualize" change activity using different metrics and methods. Some common views include the following:

- **Server.** What are all the changes over a given time period to a specific application, database, or other server?
- **Financial application.** For a given financial application and time period, do the changes meet approved criteria? What were all the changes?

- **User.** That new guy over in the break room seems creepy, and he's always wearing a T-shirt with our competitor's logo on it. Let's have a look at everything he did since he started work here.
- **Time journal.** Show me everything that happened between 5 a.m. and 6 a.m. on Christmas day when nobody else was in the building.

Validating your controls

As a final step in the testing process, you need to validate that the events you collected are consistent with the controls you are testing. This process is the same one your auditor uses. You can approach validation in two ways:

- **Control validation.** For a selected IT control, were any events detected that show the control was violated?
- **Event validation.** Does a selected event violate any defined IT controls?

When automating the testing of IT controls, focusing on seeing who is doing what and then reporting the results makes the most sense. This step can eliminate a huge amount of tedious and cumbersome effort. After you have automated testing in place, you can go one step further and automate control validation as well. We cover automated validation in Chapter 3.

The change activity data that you collect and validate will become the basis for evaluating your controls. Figure 2-1 shows a schematic representation of this concept.

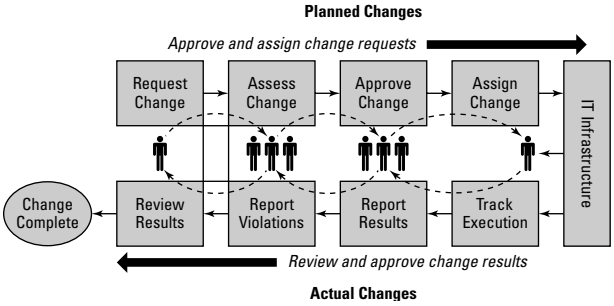


Figure 2-1: Change validation.

Chapter 3

Closing the Loop in Your Change Management Process

In This Chapter

- Following change activity to its resolution
- Benefiting from a regular self-audit
- Comparing actual changes with approved changes

"Unauthorized change" is one of the best (and worst) ways to get your auditor's attention. In fact, most IT organizations have spent considerable time and money on tools, processes, and systems to prevent unauthorized changes. In this chapter, we discuss how leveraging your existing change management tools and processes is an ideal strategy for streamlining the compliance process and preventing unauthorized changes and direct access.

Understanding Closed-loop Change Management

Simply defined, change management is a combination of tools and business processes for identifying, planning, assessing, approving, and assigning a change. Unfortunately, today's change management systems don't provide a mechanism to determine whether the change was actually completed. Similarly, these systems cannot provide visibility into changes made outside the change management process.

While change management deals with "what is supposed to happen," your audit efforts are all focused on "what really did happen." If you've incorporated automated testing (refer to Chapter 2), you have a complete record of what really happened. However, what's missing is some way to determine whether the observed action correlates to an approved change request.

Closed-loop change management is an audit strategy that combines "what is supposed to happen" with "what really did happen" to cover your complete change management lifecycle, from request through execution to review and completion.

More specifically, closed-loop change management compares *actual* changes against *approved* changes.

Another way to think of closed-loop change management is as an automated self-audit. Your goal is to more accurately verify approved changes, detect or prevent unapproved changes, and over time standardize and improve how changes are performed.

Closed-loop change management makes every change request a test and validation of the IT change control process. This includes

- **Reports of approved changes and verification that they were performed.** Simply approving a change is not enough. Your audits should also show that approved changes were actually carried out.
- **Reports of unauthorized activities and their remedies.** Besides seeing approved changes, the auditor is equally concerned with seeing unauthorized activities — and that new mechanisms were instituted to remedy those unauthorized activities.

So How Do You Do It?

You can implement a closed-loop change management system in one of two ways:

- You can manually review and audit change activity with approved change requests. Preferably, this method is supported by the automated data collection tools discussed in Chapter 2.
- Alternatively, you can create an automated closed-loop solution by integrating data collection and audit testing tools with your existing change management system.

Chapter 4

Managing Your List of Controls

In This Chapter

- Putting a stop to control creep
- Your auditor is your friend (really)
- Focusing on necessary controls

Under pressure during their first audit, many IT organizations implemented more controls than were really necessary. Excessive controls ultimately require a lot of extra work and testing to manage for future audits.

This chapter is about looking past the tip of your nose and taking a wider view of your controls. You can't afford to spend time documenting and testing controls that aren't necessary.

Focusing Compliance Requirements

The Securities and Exchange Commission initially interpreted Sarbanes-Oxley to require IT organizations to audit *all* of their internal controls. When the final version of SOX was released, that requirement was narrowed to only those controls that directly affected financial

reporting. How does the IT organization determine which controls directly affect financial reporting? The answer can be confusing.

Different answers for different organizations

Suppose you have an open port on your firewall. If you don't conduct a lot of e-commerce — for example, if you are a lumber company — a chain of events where the open port would end up affecting the financial statement is unlikely. However, if you are eBay, you can quickly see the risk. The bottom line is that all controls aren't created equal for every company.

Establishing wide-reaching general IT controls is, of course, a good idea. But doing so isn't necessary for SOX compliance. However, many internal auditors and consultants, whose primary objective was to keep companies out of trouble, adopted a "better safe than sorry approach" and often encouraged more controls than necessary. Remember, this was the dawn of SOX, and the legislation was subject to interpretation.

Many external auditors, wary of being ultimately blamed for a failed audit, would be unlikely to suggest that a particular control is unnecessary. This situation can get out of hand. More controls mean more work and cost for IT, more potential for errors, and more work for the auditor — resulting in minimal gains for SOX compliance.

Reining the controls back in

A key strategy for sustainable compliance is to identify the minimum number of controls that are needed to

verify that everything is working as it should be. For example, if you're worried about a fire in your kitchen, don't put a smoke detector in every room of your house. Establish controls where they are needed and will be effective.

We can't tell you which controls are unnecessary — only your internal and external auditor can. However, amid all the frenzy, you can easily lose sight of the big picture. Carving out a bit of breathing room to take a wider view of your controls and ask a few important questions is well worth the effort. Which controls actually matter? Which steps are actually necessary? Is there a reasonable possibility that a violation of a specific control could cause a misstatement of finances?

The requirements of SOX are specifically related to financial accuracy — don't assume that all general computer controls need to be included.

See if you can establish a direct relationship between what the auditors are looking at and financial reports. If you can't find a link, tell the auditor that you want to talk. By working with your auditor to refine and define control points, you may be able to reduce everyone's workload, simplify the audit, and get back to business.

Other ways to reduce unnecessary controls are to test, retest, filter data, and view data from multiple perspectives (refer to Chapter 2). Doing so can help determine which controls are actually necessary. You may find some duplication or redundancy.

Chapter 5

Tackling the Most Common IT Control Deficiencies

In This Chapter

- Limiting access to the right "boxes"
- Managing changes
- Improving compliance through self-auditing

As you established controls for your last audit and conducted your internal audit, you most likely discovered gaps in your IT controls. This was good news if you found these gaps before your auditor did. If you didn't, then you joined a long list of companies that ended their audit with control deficiencies. The major audit firms have identified a short list of common IT deficiencies found during the first SOX audit:

- **Lack of access controls**
- **Excessive access to systems and databases**
- **Improper change management**
- **Inadequate segregation of duties**
- **Lack of self-assessment process**

When approaching your next audit, focus on the common IT control gaps identified by the auditors. If the auditor found a common set of gaps at other companies, you can be sure that they'll dig into similar areas when conducting your external audit. Some of these areas are resource intensive and great candidates for automation as discussed in Chapter 2.

Keeping Access Consistent and Properly Controlled

With any of your systems, whether part of the IT infrastructure or end-user financial applications, proper access procedures are probably the most important controls you can implement. If someone can't access something, they can't change it — it's that simple.

Keeping people out of "boxes" they're not supposed to be in

A frequent gap in access administration procedures is a lack of appropriate controls or consistency. That is, people can access "boxes" they are *not* supposed to be in. Common causes for this type of control gap are

- **Job-change related.** Inadequate controls are in place to delete or change access when an individual leaves a job or changes job responsibilities. This type of control is especially important for contractors, who may not know a system as well as permanent employees. Even without malicious intent, they may inadvertently make changes that shouldn't be made.

- **Inappropriate approval of access changes.** Changes in access permissions for individuals, groups, or roles within your IT organization need to undergo adequate approval. That is, access to change someone's access needs to be properly controlled.

Although ultimately the point is to keep people from making changes that are inappropriate or fraudulent, from the auditor's perspective even the *ability* to access sensitive data or areas of your systems is cause for alarm.

Eliminating excessive access to systems

Excessive access refers to access to systems outside a person's role, responsibility, or approval authority within your organization. Excessive access also refers to being able to make changes during inappropriate time windows. Common gaps in this type of control include

- **Privileged access to operating system, database, and application environments.** Some users do not need access beyond the front end of their applications. Administrators do not need access to the front end where they can make changes to data.
- **Application developers and DBAs have access to production servers.** Application developers and database administrators need to work with the systems that use sensitive data, but need to be kept out of the data itself.

Sometimes the auditor views the database separately and will consider your change control procedures, access control, and database as separate concerns.

Even though it may seem tedious to have a highly structured environment where only certain employees can make certain changes, these highly defined and segregated roles are what keep your changes traceable and your auditor happy.

Improper Change Management

Change management has always been a sticky subject within IT organizations — this is still the case after the first round of Sarbanes-Oxley audits. Common change management deficiencies include

- **Frequent changes occurring outside of the change process.** Some companies estimate that up to 50 percent of the changes within their environment are conducted without obtaining the appropriate approvals through their change management system. Aside from the downtime and system vulnerability risks, an unplanned change can be cause for a serious material deficiency.
- **Inability to validate whether changes were actually completed.** Most IT organizations have little visibility into validating planned changes and whether the work was actually completed.
- **Change control processes not in place.** During the first round of SOX audits, many companies were forced to document their change management procedures for the first time. Following the suggestions in Chapter 3 is one way of addressing these deficiencies.

Inadequate Segregation of Duties

Segregation of duties is a basic, key internal control and one of the most difficult to achieve. At the most basic level, segregation of duties means that no single individual has control over two or more phases of a transaction or operation. You need to assign responsibilities in such a way that a crosscheck of duties exists. For example, look for major conflicts like a helpdesk administrator having administrator access to the network.

As a component of a compliance effort, very few companies have implemented proper segregation of duties. Proper segregation of duties ensures that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business.

Proper segregation of duties provides two benefits:

- Deliberate fraud is more difficult because it requires collusion of two or more persons.
- Innocent errors will more likely be detected.

Lack of Self-Assessment Process

Due to time and resource constraints, many IT organizations lack a regular process to verify that controls continue to be adequate and effective. Unfortunately, ignoring self-assessments is like putting off cleaning out the refrigerator — the longer you wait, the more you create messy work for yourself.

When audit time arrives, most companies are thrown into crisis mode through a lot of needless work simply because the records that would have been generated from regular self-assessment don't exist.

The lack of a self-assessment process is a red flag for an auditor. Controls that have been regularly tested and documented require far less testing by the auditor than those that have not been tested through self-assessments.

Regular self-assessment helps in all parts of compliance that are covered in the rest of this book: determining which controls are necessary, keeping your auditor happy by addressing errors in a timely manner, and ultimately reducing the effort required at time of audit.

Automation is your single biggest ally in the effort to implement a regular self-assessment process (refer to Chapter 2).

Part II

The Part of Tens

In this part . . .

Deriving as much benefit as possible from compliance can provide a competitive advantage. The first chapter in this part lists ten ways you can make your compliance strategy an opportunity instead of a drag on your time and resources. The second chapter gives a quick list of ten tips to keep in mind as you go forward with your compliance effort.

Chapter 6

Ten Ways to Leverage Compliance as an Opportunity

In This Chapter

- Getting your just reward
- Tackling operational issues
- Planning for your next IT audit
- Reaping the benefits of compliance

Compliance requires time and effort from your IT organization — you deserve a reward for your hard work. In fact, compliance can be the opportunity to tackle some of the ongoing operational issues that have hindered your IT group for years. As you plan for your next IT audit, consider these ten benefits that compliance can bring to your IT organization.

- **Improve IT operations.** IT processes are going to be the focus of every IT audit. Use compliance as an opportunity to test and fine-tune your IT processes. In doing so, you can build a stronger foundation for day-to-day operations.

- **Improve change control.** Change management has always been a major sore spot within the IT organization. With compliance, you now have the budget and mandate to purchase the tools and implement the processes to fortify your change management system and prevent unauthorized changes.
- **Improve uptime.** Through improvements in change management and ongoing operations, IT organizations reduce the risk of unauthorized changes — the prime culprit of unplanned downtime.
- **Increase accountability.** In a compliance world, everyone is accountable for their actions. Auditors want to know who is associated with unauthorized changes or direct access, or noncompliance with a policy.
- **Leverage automation to reallocate resources.** Leveraging automation to streamline the compliance process gives IT organizations an opportunity to reallocate "bodies" to more strategic IT initiatives. The compliance process is also an opportunity to assess where automation can be used to reduce risk, such as automated change validation systems.
- **Reduce costs.** Improved processes and controls ultimately reduce problem resolution times and unplanned downtime, and streamline ongoing operations. These improvements have a direct effect on the bottom line by reducing ongoing IT costs.

- **Attain closer alignment with IT and the business.** The compliance process graphically illustrates to the IT organization its value and impact to the business.
- **Improved security.** Automating access controls helps enforce information security policies, such as limiting access to sensitive data to authorized users.
- **Increase your overall compliance score.** Compliance isn't only about Sarbanes-Oxley. A host of other compliance requirements exists, such as HIPAA and Graham-Leach-Bliley. Strengthening change and direct-access controls strengthens your hand with other health, financial, and federal compliance requirements.
- **Gain competitive advantage.** Your competitors face the same compliance challenges. Ultimately, the company that does it right the first time gains a distinct competitive advantage. The company that gets it wrong, wastes time, resources, money, and potentially public prestige if its material weaknesses result in a restatement of earnings.

Chapter 7

Ten Ways to Create a Sustainable IT Compliance Program

In This Chapter

- Sustaining your compliance strategy
- Saving time and effort

A sustainable compliance strategy evolves as requirements evolve, and saves you the most time and effort. The following ten tips steer you in the right direction.

- **Automate.** Use automated tools to verify and audit change activity. This will save time, money, and resources (headaches, too), and increase the accuracy of reporting.
- **Evaluate and adjust.** Compliance is an ongoing process. Regularly assess IT control effectiveness.
- **Self-assess.** At least quarterly, companies should self-assess their change control processes.
- **View compliance as an opportunity.** Compliance should be approached as an opportunity

to improve core IT and operational processes — not an extra piece of work to adhere to some federal legislation in Washington, D.C.

- **Be practical.** Compliance is not created overnight. Take a methodical approach to create a solid foundation for a sustainable compliance program.
- **Understand financial flows and business effect.** Knowing the business effect of the IT infrastructure is extremely important. Effective IT organizations are cognizant of the relationship between their actions on the infrastructure and the effect on financial flows and the overall business.
- **Manage your controls.** Many controls that were created during the first round of audits may be unnecessary. When testing, evaluate whether they're truly material to the financial systems and inform your auditor of any concerns.
- **Leverage existing tools and processes.** Most companies have already invested in change management and access control processes and tools. Leverage the capabilities of these in your compliance program. For example, extend your change management system to create a closed-loop solution that verifies and validates actual change activity.
- **Use metrics to test controls.** You can't measure what you can't see. Use tools to gain visibility into your critical IT controls, such as change management and direct access. These metrics will be the core of your IT control tests.
- **Don't reinvent the wheel.** Use standards such as COBIT and ITIL to create your sustainable IT compliance program.