Compliments of QUALYS®

IT Policy Compliance FOR DUMMIES®

Your quick guide to IT policy compliance

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Jason Creech
Matthew Alderman

IT Policy Compliance FOR DUMMIES®

by Jason Creech and Matthew Alderman

WILEY

A John Wiley and Sons, Ltd, Publication

IT Policy Compliance For Dummies®
Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

ISBN: 978-0-470-66535-0

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Introduction

Welcome to *IT Policy Compliance For Dummies*! Compliance is a big fact of life for many organizations. At the core, it mostly concerns obedience to laws and regulations, especially regarding the use of information technology (IT). This book is all about understanding IT policy compliance, and discovering how your organization can use technology and business processes to fulfill compliance requirements set by government, industry, and your Chief Executive Officer (CEO).

About This Book

This book simply explains IT policy compliance and the steps your organization needs to carry out to prove compliance to an independent auditor. After reading this book you'll know how to create compliance policies and prepare your IT operations to fulfill those requirements.

Foolish Assumptions

In writing this book, we assume that you:

- Work in a mid-to-large sized organization and know that you have to comply with policies, but you aren't sure what's required or what you need to do.
- Are familiar with information technology and managing its operations.
- Want to discover the easiest, most effective and direct way to prove compliance with policies.

How to Use This Book

This book is divided into five succinct and easily-digestible parts:

- **Part I: Stepping Into the World of IT Policy Compliance.** Start here for a primer on the meaning of policy compliance and its relationship to IT.
- **Part II: Defining the Problem of IT Policy Compliance.** Here we direct you to the alphabet soup of regulations and standards and look at how they relate to policy compliance.
- **Part III: Best Practices for IT Policy Compliance Management.** This part serves up a swift orientation to the guts of IT policy compliance, including ten best practices.
- **Part IV: Looking at Automation in IT Policy Compliance.** Here you discover how automation can help your organization ease policy compliance and save money.
- **Part V: Ten Tips for IT Policy Compliance.** Follow this short list of steps to ensure compliance with regulations and standards.

You can dip in and out of this book as you wish. However, although you don't have to read this book from start to finish, the topic will make more sense if you tackle it in sequential order.

Icons Used in This Book

We highlight crucial text for you with the following icons:

This icon targets hints and shortcuts to help you comply with policy.

Memorize these pearls of wisdom – and remember how much better it is to read them here than to have your auditor give you a know-it-all lecture later on.

The bomb means 'whoops.' It signals common errors that can happen. Avoid these at all cost.

Prepare for a little bit of brain strain when you see this icon. But don't worry – you don't need to have a doctorate in policy to successfully pass a policy compliance audit.

Where to Go from Here

Check out the section headings in this book and start reading wherever it makes sense. This book is written with a sequential logic, but if you want to jump to a specific topic you can start anywhere to extract good stuff.

Part I

Stepping Into the World of IT Policy Compliance

In This Part

- Setting out the meaning of policy compliance
- Defining the compliance ecosystem
- Understanding the importance of IT policy compliance
- Demonstrating your conformance with laws and regulations

According to the dictionary, *compliance* is 'conformity [or] acting in accordance with accepted standards.' For example, driving according to the speed limit is an act of compliance, as is carrying just one piece of hand luggage onto an airplane. A DVD player manufacturer who adheres to technical manufacturing specifications of the discs is also complying with a set of standards. Compliance can also entail following a set of rules or 'guardrails' within which your organization can 'legally' operate. The implementation of such procedures for compliance may entail a variety of standards.

In practice, most people equate compliance with conformance to laws. Laws and regulations surround our lives. These range from the pharmaceutical laws that protect against untested and unsafe medicines, to US Federal Deposit Insurance Corporation (FDIC) regulations that insure the safety of bank deposit accounts up to $250,000, to environmental laws aimed to protect the health of people and the world in which we live.

Organizations have a variety of laws requiring compliance. Examples of typical details from these laws include:

- Tax laws (federal, state, and local).
- Employment laws (workplace safety, unemployment, health insurance, and so on).
- Consumer protection laws.
- Data protection (in other words, information security) laws.

Policy Compliance 101

This book is about compliance – specifically, IT compliance – for organizations of all sizes, including commercial enterprises, government agencies, and public-sector entities. *IT policy compliance* is the implementation and management of information technology in accordance with accepted standards. We describe some of these standards in Part II.

The applicability of standards to your organization depends on a variety of factors, including:

- The nature of your business.
- The types of data being processed by your organization.
- The risks that apply to your environment.

However, don't fall into the trap of assuming that IT compliance is just about technology. IT policy compliance is a complete ecosystem that includes:

- Organizational strategic objectives.
- User awareness and training.
- High-level policies.
- Procedures and standards.
- Configuration settings.
- Technology controls.
- Ongoing monitoring.
- Business risk assessments.
- Internal and external auditors.

Above all, however, compliance is about people, processes, and technology. Many companies put too much emphasis on the technology and end up failing audits due to their lack of attention on people and processes.

While IT makes this compliance ecosystem more complicated, using the right approach can help a company to automate its controls and controls monitoring. Benefits include being able to:

- Monitor a larger range of transactions, controls, and systems than a person could ever assess using a manual process.
- Provide a level of consistency that eliminates the subjectivity of human review.
- Run metrics and reports that ultimately help you manage the quality of both your compliance program and operations overall.

We explore these topics further throughout this book, diving deeper into compliance, best practices, and the role of automation.

Focusing on IT Compliance

Because IT controls are just one aspect of being compliant, you may ask why IT compliance is such an important topic. The answer is, quite simply, that it's because the vast majority of business and government today is done through or with information technology. This ranges from using an e-commerce site for taking orders from customers online, to a bricks-and-mortar business using software for back-office accounting and order management. Organizations are run with IT, and this brings unique operational risks. Those risks can bring widespread negative impact, and that's what captures the attention of policy makers of laws such as Sarbanes–Oxley ("SOX").

We discuss the Sarbanes–Oxley law, and specifically Section 404, in Part II, but as we point out there, even this famous law does not mandate IT audits. SOX does require a multitude of new controls for auditing internal controls but, because

financial reporting is run on IT, it follows that these controls are for the benefit of meeting requirements of Sarbanes–Oxley! Our goal in this book is to take regulatory requirements that relate to industry-standard concepts and align them with IT for no reason other than that's what your business needs. Applying policies to complex IT systems and architectures is the true challenge of IT policy compliance.

Proving Conformance

An important aspect of policy compliance is proving IT operating conformance with laws and regulations. In its current state, most IT compliance requirements start at the top with laws and regulations. These articulate the 'policies' governing their requirements. Policies, in turn, have their own operating requirements for compliance that are pushed down on each organization. Examples include the Sarbanes–Oxley Act, to regulate financial reporting, and the Gramm–Leach–Bliley Act, to regulate non-public personal information, including financial data. These laws are either translated into, or make reference to, standards for IT implementation and ongoing management.

Conformance with some broad standards, such as those from the US National Institute of Standards and Technology (NIST) or the International Standards Organization (ISO) can provide near or even simultaneous compliance with IT requirements of multiple laws and regulations. Organizations that start by doing the right thing, and make reference to internationally adopted standards, can earn compliance as a by-product of a quality and controlled operational environment – and not simply for the sake of putting an 'X' on a legal checklist. In a word, compliance can trigger business benefits that transcend obedience to the letter of the law.

Part II

Defining the Problem of IT Policy Compliance

In This Part

- Wising up with a brief history of policy compliance
- Looking at auditor interpretation and ambiguity
- Wading through the alphabet soup of regulations and standards
- Making sense of IT policy compliance

Policy compliance has always been part of doing business. The financial industry, for instance, has lived under regulation since the creation of financial markets. Industries such as healthcare and pharmaceuticals have heavy oversight, as do many other business sectors.

The key to compliance is understanding the structure of regulation and knowing how to play your role in it. This part makes that simple.

A Brief History of Compliance

The first thing to know about policy compliance is that any regulation or standard (especially in the US) is typically a reaction to some sort of negative event. For example, the US Securities and Exchange Acts that dramatically overhauled the securities markets in 1933 and 1934 were passed in response to the stock market crash of 1929. The resulting policy created by the US Congress increased scrutiny and reporting requirements. The policy presumed that investors would thereby get more accurate information and make more careful decisions. And they did, at least for the next half-century.

Reacting to the specter of data breaches

The news is filled with a non-stop stream of reports about data breaches – from large retailers like TJMaxx, to an array of universities and other public-sector organizations, and to companies like Equifax who are in the business of handling personal information. Hundreds of other similar stories have been reported about botnets, Russian Mafia hackers, viruses, and worms.

The Privacy Rights Clearinghouse keeps a running total of data breaches involving computer records that contain sensitive personal information. As of February 2010, more than 345 million records in the US alone have been involved in security breaches (for details, see `www.PrivacyRights.org`). To the casual observer, therefore, it may appear that no computer data is safe from exposure. For that reason, policy makers have reacted with laws and regulations requiring compliance with controls to protect sensitive personal and financial data.

In the 1990s, laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Financial Services Modernization Act – aka the Gramm–Leach–Bliley Act (GLBA) – were passed in the US to protect the privacy of personal data. Each of these regulations has specific requirements for the protection of Personally Identifiable Information (PII). In addition, both of these regulations require annual risk assessments to determine compliance with the requirements. For GLBA, the audits are performed by auditors from the government agency that oversees a particular bank. Examples of these agencies include the Federal Reserve Bank (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the National Association of Credit Bureaus (NACB).

In the 2000s, some policy makers believed that the collapse of two large public corporations – Enron and WorldComm – could have been identified and prevented had appropriate controls and accountability measures been in place. These, and several other less-publicized meltdowns, triggered the passage of the Sarbanes–Oxley Act in 2002.

While the majority of 'SOX' (as the U.S. Act is often called) focuses on financial reporting and corporate director accountability, a key component for IT professionals is the inclusion of Section 404. This section mandates public companies to adopt, audit, and report on their internal controls related to financial reporting systems. While the language of Section 404 isn't IT-specific, it's obvious that most controls in modern organizations are either managed or monitored with information technology. Policy compliance, therefore, frequently relates to the use of IT.

But Isn't SOX Section 404 Just One Paragraph?

The answer to this question is, 'yes,' and herein lays a typical challenge of compliance. Section 404 of the Sarbanes–Oxley Act is a single paragraph of less than 75 words. Nevertheless, that tiny set of words has led to many public companies hiring two sets of accounting firms and spending, on average, $1.7 million on Section 404 compliance. The reason for this response lies in the ambiguity associated with regulations like SOX Section 404. The wording of laws is meant to be universally applicable to a broad range of companies, which almost guarantees they are vague and non-prescriptive.

The critical question to ask is: who determines how a paragraph like Section 404 translates into a clean audit opinion by an accounting firm? Ultimately, audits are signed by the public accounting firm, and this is why companies employ two such firms – one to advise and one to audit. Standards bodies have stepped in to help by providing intermediary guidance, bridging how the law reads and specifying a specific related control (such as, for example, how many characters should be in a password). This has helped the accountants to promote and maintain consistency among licensed Certified Public Accounting (CPA) firms, something the industry learned over 100 years ago that was vital for sustaining faith in the profession.

Regulations vs. Standards vs. Auditors

Navigating your way through the hierarchy of regulations, government and industry standards, and audit methodologies can be difficult. Figure 2-1 sets out the framework in black and white:

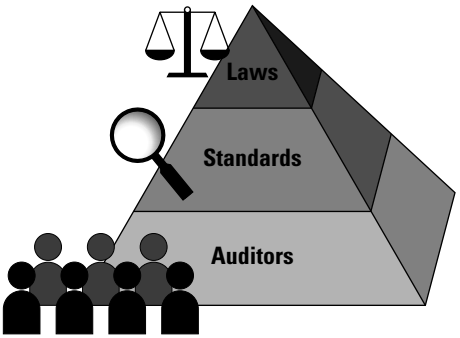


Figure 2-1: Laws, standards, and auditors framework.

To put this diagram into simple terms, organizations must comply with laws. These organizations use standards as guidance for operational policies used to comply with the laws. Those same standards, combined with related methodologies, are the basis used by auditors to test policy controls and certify compliance.

Here are some examples of areas of responsibility and the related laws that affect IT policy compliance:

- Financial reporting and accountability: Sarbanes–Oxley Act of 2002.
- Non-public personal information, including financial information: Gramm-Leach-Bliley Act of 1999 (GBLA).
- Protected health information: Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Energy regulation and authority of federal agencies such as U.S. Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC): Energy Policy Act of 2005.
- Personal information breach notification: California SB 1386 and the American Recovery and Reinvestment Act of 2009 (ARRA).
- Government computer security: Federal Information Security Management Act of 2002 (FISMA).
- Personal data: UK Data Protection Act of 1995.

Some example sources of government and industry standards that affect IT policy compliance include:

- Control Objectives for Information and Related IT (COBIT).
- National Institute of Standards and Technology (NIST) standards.
- International Standards Organization (ISO) 27001.
- Information Technology Infrastructure Library (ITIL).
- Payment Card Industry Data Security Standard (PCI DSS).
- NERC Critical Infrastructure Protection (CIP) standards.
- Federal Financial Institution Examination Council (FFIEC) Information Security Book.
- Security Content Automation Protocol (SCAP).

Examples of government- and industry-certified auditors responsible for verifying IT policy compliance include:

- Internal auditors employed by an organization.
- Certified Public Accountants (CPAs).
- Bank auditors, such as those from the Federal Reserve, Federal Depository Trust Corporation (FDIC), and Office of Comptroller of the Currency (OCC).
- Payment Card Industry (PCI) Qualified Security Assessors (QSAs).

PCI: A global standard for securing payment card data

No compliance driver has impacted IT teams more than the Payment Card Industry Data Security Standard (PCI DSS). The five major payment card brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. – forged this standard in 2004 to combat payment card fraud and prevent the theft or unauthorized use of cardholder data. The standard applies to all entities that store, process, and/or transmit cardholder data.

Unlike the Sarbanes–Oxley and Gramm–Leach–Bliley acts, the PCI standard is largely prescriptive. It includes detailed, defined technical and operational controls for protecting networks, systems, and components used for processing payment cards. For more information about the PCI standard, please read our book, *PCI Compliance For Dummies*, also written by Qualys.

Typically, the ultimate determiner of compliance is the auditor that tests an organization's IT controls for specific laws and standards. Remember, though, that auditors are human and can reach different conclusions about compliance from the same set of audit data. For this reason, companies not only must attempt compliance – they must be able to prove it.

Making Sense of It All

To get to the bottom of IT policy compliance, you need to know the answers to these questions:

- What law(s) apply to my company or agency?
- What standards help to guide us toward compliance with those laws?
- What type of audits and assessments are required for compliance?

- What controls do we need in place to meet policy requirements?
- What evidence do we need to substantiate compliance to auditors?

In general, most security and audit professionals say that compliance is easy if you have a good policy and control framework in place. In theory, this sounds promising. However, it doesn't take into account the variability in auditor perspectives, so the mere fact of having controls in place is not enough. To quote Tom Cruise from the movie, *A Few Good Men*, 'It doesn't matter what I think, it only matters what I can prove.' The same holds true in the world of IT policy compliance auditors.

Compliance outside the US

While laws and standards such as Sarbanes–Oxley and PCI have drawn significant attention, the US did not invent IT policy compliance. The European Union, for example, passed its Data Protection Directive in 1995. Swiss banks are well known for their Bank Secrecy Laws, and countries like Germany (which has had privacy laws since the 1970s) view an email address in the same manner that someone in the US would view their unlisted phone number. Policy compliance is a global issue.

Part III

Best Practices for IT Policy Compliance Management

In This Part

- Keeping a balanced perspective on IT policy compliance
- Understanding the auditor's perspective
- Aligning IT compliance/security with business processes
- Building an IT compliance policy and controls environment
- Establishing and monitoring accountability
- Using risk-based prioritized remediation of control weaknesses

Much as you might wish otherwise, the requirements of IT policy compliance aren't going to go away. If anything, requirements for compliance will continue to become more complex and demanding over time in response to negative events. With this in mind, IT and security managers have to stay composed, maintain a balanced perspective, and adhere to a plan that makes policy controls within the environment effective and demonstrates compliance in a straightforward manner. You need your compliance framework to flow through the organization in such a way that people know their responsibilities and are held accountable for their actions.

This part offers you practical guidance and best practices for achieving those ends through IT policy compliance management.

Best Practice #1: Remember the Big Picture

The goal of an IT policy compliance framework is not to be compliant merely for the sake of compliance, but to make your organization's operations secure and effective, and to ensure they run in harmony with the underlying objectives of policies that underpin the framework. In other words, always remember the big picture. This may sound obvious, but you'd be amazed how many organizations plan their IT controls around strict adherence to compliance requirements – and completely miss deploying key controls that leave the organization open to attack or misuse. Not only are these organizations vulnerable to harm, they are, by default, non-compliant! As proof of this, several well-publicized security breaches have occurred within organizations that, on paper, had been certified as 'compliant.'

Maintaining your perspective

Maintaining your perspective starts with understanding your organization's policy control objectives. This is a fancy way of saying, 'What are you trying to protect or control?' Examples of high-level control objectives for IT policy compliance include: data protection and information security; fraud prevention; errors and omissions; and technology failure.

You also need to understand the types of controls that make up your compliance universe. Companies often focus only on controls for data security and overlook other key areas such as:

- *Administrative controls:* policies, procedures, and processes associated with the control objectives.
- *Physical and environmental controls:* the physical protection of electronic and non-electronic information or assets. Examples are door locks, camera monitoring, and fire suppression.
- *Logical controls:* the control of access to specific networks and resources by an authorized user; generally managed by information technology.

Aligning or mapping the controls to the alphabet soup of standards and regulations that we discuss in Part II is a useful practice. Mapping frameworks can help with this process. Most Certified Public Accountant (CPA) firms maintain a mapping framework to guide the use of their own methodologies. In addition, you can purchase and adapt data sources such as the Unified Compliance Framework (UCF) for control guidance and help with keeping up with changes to regulations and standards.

Understanding the auditor mentality

The auditor is the ultimate 'Monday Morning Quarterback.' Their role is to render an opinion on whether or not your organization's policy controls are working, and if they were designed properly before deployment.

An auditor begins an audit by studying your control design. Auditors want to know what the objectives are and how they align with your business, the day-to-day processes you employ, and the underlying technologies you use.

An auditor plans his/her activities by evaluating audit risk. *Audit risk* is the risk that an auditor has incorrectly issued an unqualified (or clean) opinion on a set of financial statements or a control environment. Audit risk is defined as follows:

- Audit risk = Inherent risk × Control risk × Detection risk
- *Inherent risk* means things that are built into the audit situation and that the auditor doesn't control, such as type of business, type of activity, or other environmental factors.
- *Control risk* refers to the likelihood that the control environment won't detect or prevent an error or misstatement. When the client designs a better control environment, it automatically reduces control and audit risks.
- *Detection risk* is the likelihood that an error or misstatement won't be captured by an auditor's testing. This area of audit risk is the one over which an auditor has the most control.

Be aware that an auditor's objective is to minimize overall audit risk. If inherent risk and/or deficiency are present within the control environment, the auditor compensates by reducing detection risk. As a result, the auditor does more testing and uses larger sample sizes.

In summary, if you don't have a well-documented control design, expect the auditor to do a lot of testing.

The auditor uses this approach to plan a sampling methodology. Practically speaking, an audit cannot check every IT control of every asset. A sampling methodology limits the checking to an acceptable scope by specifying the number of systems, transactions, and so on, to be tested to obtain a reasonable determination of whether or not your controls are meeting your policy objectives.

Note that the types of controls you implement also affect the type of testing that occurs. For instance, if you configure your servers manually and audit them manually, the auditor has no choice but to do so as well. Likewise, if you use automated configuration management software and automated compliance monitoring technology (such as QualysGuard Policy Compliance), auditor testing will focus more on the configuration of the technology, plus a light manual review to insure that the technology is working properly. While auditors are supposed to have no preference for what type of technology you use, the adoption of such technologies at other companies can only help to increase the auditor's confidence in the effectiveness of what that technology is controlling.

What if you fail?

Rightly or wrongly, another source of auditor perspective is the results your organization obtained from previous audits. Failing audit tests once can be a mark against your organization, but failing twice can really impact its credibility. Failed audits almost always trigger an increase in scope for future audits. In the worst case, they can lead to potential financial penalties for the company, its directors, or individual officers. Top executives can lose their jobs by failing an audit due to a known issue that was never resolved.

You have to prove it!

Passing an audit is all about what you can prove. If you have a risk- or financially-based remediation process (described in the 'Best Practice #8: Prioritize Remediation Activities' section later in this part) that justifies why you didn't implement a particular control, your audit position can be fine. Just be sure to document those decisions – and do so consistently. Auditors have a higher degree of confidence when their audit clients can show that the compliance program is part of a daily process as opposed to a once-a-year or quarterly event.

"An auditor's perspective"

I am a Certified Public Accountant at a national CPA firm where I perform Sarbanes–Oxley, SAS 70, Payment Card Industry Data Security Standard, and other types of IT audits. Clients come in different shapes, sizes, and states from a policy controls perspective. The easiest audits for me are when it's clear that the client has a continuous and consistent compliance program. I have some really great clients who generate monthly reports to show that they monitor their compliance with tools such as QualysGuard Policy Compliance, and they make those reports available to me. The reports are hard evidence that a client has the required policies and procedures – and that they actually follow them. From an auditor's perspective, it's clear that organizations like these take compliance seriously and that they employ a systematic process for holding themselves and their IT staff accountable. With these clients, I am typically 'in and out' in a matter of days.

And then I find some clients who clearly view my audit as a once-a-year activity. They do a lot of preparation to try to convince me otherwise by shoveling in a mound of paperwork, but I know better. The results are simple. As I'm less confident in their control environment, I'm forced to test it with a higher sample rate, and that comes at a higher cost to the client. The extra scrutiny inevitably reveals more problems. Sometimes the end result is a qualified report that the client doesn't like, and I don't like having to issue.

Simply using IT policy compliance products for continuous control monitoring doesn't automatically make audit issues go away. But use the right tools under the right policy framework, stay consistent, and keep your reports, and you can reduce, by orders of magnitude, the amount of money you spend every year in audit fees – and the amount of pain and sweat you go through!

Best Practice #2: Align IT Policy Compliance and Security with the Business

That compliance has to align with the business is good advice, but how do we move beyond the rhetoric and do something useful with this advice?

Real business and compliance alignment starts with understanding the culture of your organization. Many models have been created to devise and articulate organizational capabilities and maturity. Figure 3-1 shows one example – the Software Engineering Institute's (SEI) Common Maturity Model for Integration (CMMI). (You can read more about it on the SEI website at `www.sei.cmu.edu/cmmi`.) Another example is the Microsoft Corporation's Service Oriented Architecture (SOA) Maturity Model. A lot of thought, plus years of research, went into building these models, and yet both boil down to just one idea: specifying the operations of an organization.

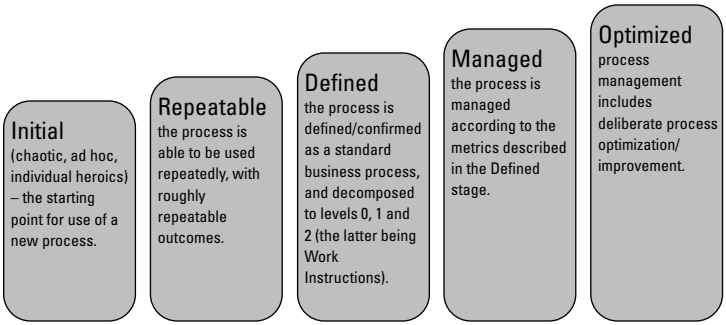


Figure 3-1: The SEI Common Maturity Model.

At one extreme of the Software Engineering Institute Common Maturity Model, you have organizations labeled *Optimizing* or *Dynamic*, defined as having a self-sustained process-oriented organization. Less than one percent of all organizations fall into this category. At the other extreme you have organizations called *Initial* or *Ad-Hoc*, or what some

ever refer to as 'Chaotic.' This category applies to organizations that live and breathe by the heroics of key individuals and leaders – anything but process!

You might then ask what all this organizational theory has to do with IT compliance. Aligning business with compliance starts by understanding the type of organization you're in and, most importantly, what has the best chance of working within that environment. Approximately 40 percent of organizations fall into the 'ad hoc' or 'chaos' classification, so if you think that label fits, your organization is normal. For policy compliance, this means your organization will typically have to design more controls that are preventive and detective in nature. Simply issuing a policy and hoping it will be followed is a recipe for failure. Organizations in this category may not require in-depth policies, but detailed standards for configuration and implementation with technology controls are what will keep them aligned and in compliance.

After you determine what level of control aligns with your organization's culture, the next step is to address the business risk. One of the key historical challenges here is that IT audit data typically focuses on the individual IT technical asset (or set of systems) under review. For policy compliance, the focus of reporting must be the business process layer or the specific business risk you're trying to assess. Here are some examples:

- Privacy audits for personally identifiable information.
- Audits for protection of intellectual property in research and development.
- Operational reviews of controls for critical lines of business, such as e-commerce. The PCI Data Security Standard, for instance, puts the focus of an assessment on a particular segment of business operations as opposed to the overall enterprise.

A business-based approach also maximizes the value of the security data collected. These data can be useful in identifying waste, increasing the quality of IT services, and promoting efficiency and visibility into the business.

Your ability to speak about findings and risks from a business process perspective will allow the organization to better focus on planning, remediation, and communication. These data can also help justify and sustain a compliance program to the executive management of the organization.

Best Practice #3: Understand Your Technology Environment

Purists would tell you that a compliance program should be independent of any technology. In theory, they could be right, but in practice the technology footprint, like culture, directly impacts the design and effectiveness of the IT policy compliance program. Starting with design, there are a few questions that can guide your control emphasis based on how your organization approaches business and technology:

- In general, what type of environment do you have?
- Is your environment homogeneous (where things are relatively consistent)?
- Is your environment heterogeneous (where there's a good amount of everything)?
- Does your environment use traditional standalone systems or newer virtualization technology?
- Do you operate an e-commerce site?
- Do you have lots of mobile users?
- Are all of your IT assets physically located under one roof?
- Do you host applications or data at external data centers, or use cloud computing or Software-as-a-Service?

Identifying your environment

In a *homogeneous environment,* the technical environment is largely consistent. Here, you see names such as Microsoft, Hewlett-Packard, or Dell for nearly all desktops, laptops, and servers. Networking equipment is largely from Cisco Systems, Inc. and while deviations may exist, they are rare. Some

organizations that have many locations may standardize on a consistent deployment. This enables each location to have a duplicate technical environment, such as branch locations for banks or store locations for retail environments.

Heterogeneous environments use a broad range of technologies, versions, and even different compliance and security applications. The heterogeneity of the technical infrastructure often grows more complex over time, especially in large organizations. New acquisitions, mergers, and changes in IT leadership and direction are typical reasons why a technical environment can become more diverse and complex over time. In terms of compliance and security, each technology platform must have a *hardening policy* describing what must be secured, along with a description of mitigating procedures on how that system will be managed for the protection of critical information assets.

Whether you're in a homogeneous or heterogeneous environment, you should never change your policy compliance strategy. The type of environment impacts the level of effort required to implement a compliance technology, especially if you have to install agents on a multitude of platforms. In general, the cost of compliance is less expensive for homogeneous networks. Fewer technology types, fewer technology vendors, and fewer technology versions translate to fewer policies and less complexity, which results in lower cost of compliance and security per system because individual processes impact greater percentages of the IT volume.

Bearing virtualization and cloud computing in mind

Virtualization or the abstraction of IT resources is also a key force in today's market, where you have many 'logical' systems residing on a few physical ones. However, use of virtualization has added additional complexity to compliance and security initiatives. For example, the deployment of a single bad image to virtualized systems can instantly create many policy violations. Prior to virtualization, each physical device was associated with a single instance of an operating system. Now, each physical system, such as a Windows desktop with virtualization software installed, means that a physical device

may be hosting multiple 'logical' systems. These virtual systems might share the physical system's unique IP address, or each virtual 'instance' may have its own IP address on the corporate network. Obviously, the potential permutations of virtualization pose a huge challenge for IT policy compliance!

If your organization uses virtualization, your policies must cover acceptable use of the technology and authorized users of the technology should be well documented. Also, be sure to create policies for the virtualization management systems themselves and the management of the virtual images. An employee or contractor could easily copy a critical virtualized server to a thumb drive and analyze that system in the comfort of their own home. Additionally, use a staging area to test the secure image using an approved IT audit procedure. The common denominator is typically an IP address.

None of these testing procedures are required if you use a cloud-based solution like QualysGuard Policy Compliance because the hosted server is physically protected from such theft of server data.

Figure 3-2 shows an example of how a single vulnerability in a virtualized IT environment can affect many systems.

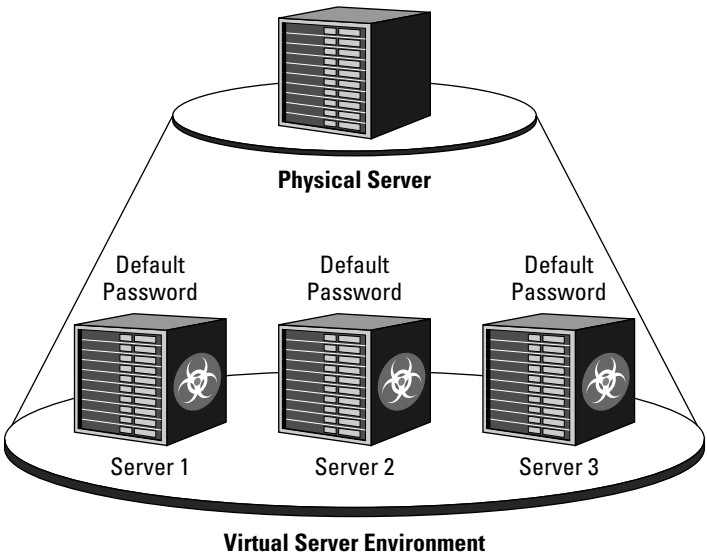


Figure 3-2: A single vulnerability is magnified in a virtualized environment.

Marketing hype aside, most agree that cloud computing, also known as 'just-about-anything-as-a-service,' is a business-driven force to be reckoned with. Using cloud-based services such as Software-as-a-Service (SaaS) has tremendous cost-savings potential, but also requires the organization to give up some of the control associated with running everything itself. It also requires you to confirm that your service providers use the same controls that you would. From a policy control design perspective, this translates to a higher emphasis on administrative controls (in other words, contracts) and slightly less emphasis on technical security controls because you're delegating management of the hosting and network systems.

Best Practice #4: IT Compliance Starts with Policy

In the preceding three sections, we describe notions of high-level control objectives, corporate culture, and technology analysis to provide a sense of what you have to work with. These, along with the standards you want to build are your elements for basic policy design.

Policies define the 'who' and 'what' elements of compliance. Procedures and standards define the 'how.' All three can be in the form of documents, or they may spring from common wisdom, such as using a known good server to build images or a Windows security policy template that can be applied to numerous machines. Just remember: developing pages and pages of policy documents that no one will read is a waste of time. Simply having a high-level policy stating that systems will be configured securely and in accordance with industry standards, or a policy declaring a configuration management system must conform to a standard such as NIST or CIS, may be enough. And remember that you must also have the ability to prove conformance to these standards.

Policy creation requires interviews with the business stakeholders to identify which controls are applicable, which are not, and what weighting should be assigned to controls and assets for prioritization and results measurement.

Compliance requires specific technical and procedural details

A common policy-driven configuration procedure for IT security is disabling telnet and file transfer protocol (FTP). The reason for this is that when connections are made across the network to a telnet or FTP service, the username and password information used to connect can be 'sniffed' from the network layer. Encrypted protocols such as Secure Shell (SSH) and Secure Copy (SCP) are commonly used as alternatives to telnet and FTP as they represent more secure ways to communicate with the target system.

Your organization needs to think about how to disable telnet and FTP processes. Is there a standard procedure for doing even this simple task in your organization? How do you educate staff and contractors on their roles in fostering policy compliance within your company? Your organization's policies and procedures should address specific questions like these.

Note that most large organizations fall under multiple regulations, so cross-mapping controls with regulations can be useful to avoid the hassle and cost of redundant testing.

Documenting corrective actions is a must. Just saying what should be done isn't enough. Policies also must include what, by whom, and within what amount of time remediation occurs.

Best Practice #5: Establish Accountability

Compliance programs don't work without accountability. Establishing *accountability* is an important but often overlooked facet of IT policy compliance management. It involves the definition of roles and responsibilities in the organization, that define what assets an individual is responsible for protecting and who has authority to make decisions.

Starting at the top

Accountability must start at the top of an organization, meaning that the executive team is the critical driver for pushing compliance across the organization. To get executives and managers onboard with compliance programs, the main tactic of yesterday's (and unfortunately still some of today's) security and compliance professionals was to scare them with stories of breaches or compliance fines. Reciting these has less effect now due to widespread coverage of breaches in the news. CEOs already know about these, so you need a stronger argument to grab attention.

A more useful angle stems from a paradigm shift where executives are beginning to see real business value from IT policy compliance:

- Reducing risk can bring true and real improvements to the bottom line.
- Security and compliance data can reveal untapped value with cost savings.

Audit procedures can often spot waste and enable you to achieve cost savings in many areas; for example, finding and deleting active user accounts for former employees on operating systems, databases, and applications, or questioning the need to purchase an additional server when the current server is only working at 30 percent capacity.

Ultimately, process excellence can – and should – lead to efficiency gains. Some of these are measurable in terms of dollars saved or staffers doing redundant tasks who you can reassign to other projects. An in-touch Chief Executive Officer or Chief Financial Officer will understand the risks and the benefits to a compliance program, and will note that what is good for managing IT can spread across the organization.

Defining roles and responsibilities

IT has two main roles: data/system ownership and data/system custodianship. The *data* or *system owner* is a member of the management team within the organization who is responsible for how data and systems are used and their ultimate care. This

owner could be the CEO or the general manager of a particular line of business. The data or system owner is accountable for managing and protecting the information.

The *data* or *system custodian* is in charge of maintaining and protecting data through traditional operational processes, and is usually staffed in IT operations or security. Making tape backups, maintaining logs, and restoring data are example responsibilities for this role. The data or system custodian doesn't decide how the data is stored or protected, but is responsible for executing decisions made by the data owner.

More specific custodial roles may include system administrator, security analyst, internal audit, legal counsel, and so on. IT security and compliance policies are especially important for these roles, and must specify who has particular authority to make particular decisions on assets and business processes. Naturally, this is easier said than done.

Improving your value to executives with policy compliance

A dreaded, but common, executive perception is that IT security and compliance are nothing but cost centers to an organization. In the current economic climate, that means that the staff in these departments is often the first to go. Being able to tell the perceived value of the IT service provided in the order of staff layoffs almost seems like a perverse game.

In reaction to this, Gartner and other industry analysts have been pushing the 'Align IT Security/Compliance with the Business' theme. This tack aims to provide executives with visibility into the value of IT to the business, and change the 'cost center' perception.

Most compliance products have been moving to risk-based approaches, which helps to prioritize remediation processes. Using a risk-based approach also translates mountains of complex, cryptic compliance and security data into three values the senior management team can understand: liability, cost, and impact.

Being able to speak the business language of executives helps you to improve their perception of your value to the organization. Policy compliance can be your friend!

An IT policy compliance solution should automate the assignment and management of roles and responsibilities. This capability is built into the on-demand solution from Qualys, called QualysGuard Policy Compliance. Figure 3-3 shows typical roles and access permissions used with QualysGuard Policy Compliance.

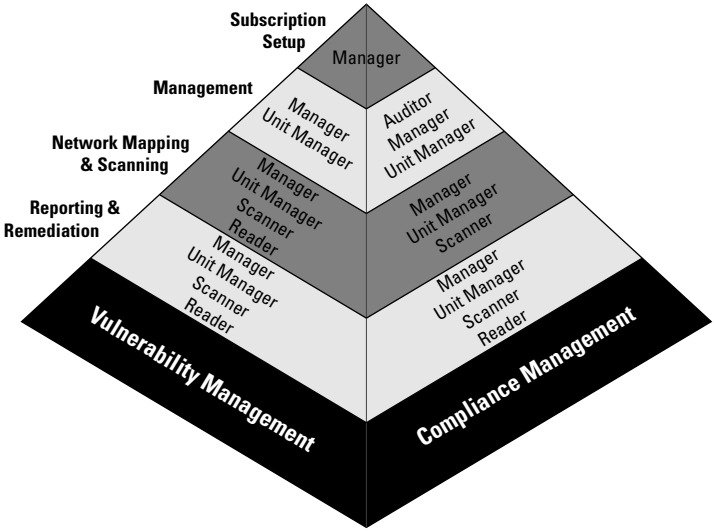


Figure 3-3: Roles and access permissions used with QualysGuard Policy Compliance.

Choosing the carrot or the stick

Many organizations struggle with a changing corporate culture to get their business units and technical staff to comply with policies and procedures. In recent years, a few interesting ways have emerged to 'encourage' the actions of business and IT leaders to be more in line with IT policies and compliance requirements:

- Management By Objectives (MBO): Many organizations now include compliance in their MBO-based incentive compensation.
- Quality Management: Building on MBO, many large organizations that adopt quality management programs

(like Six Sigma) incorporate compliance metrics into their overall metrics programs for measurement and reporting.

- Peer pressure: Many organizations publish the results of internal compliance monitoring and audits to show how departments or groups rank against each other.

The alternative to these methods is the 'stick' or threat of negative consequences when compliance is not met. Fear is a known management technique, but the most effective organizations tend to use some of the more positive approaches.

Best Practice #6: Conduct a Pre-Audit or Readiness Assessment

In the new world of post Sarbanes–Oxley compliance, some large organizations find themselves hiring two sets of accounting firms. One firm does 'pre-audits' and advises them on what they should be doing. The other firm actually performs the audits. This trend has slowed somewhat as audit requirements have firmed up, so most firms no longer need this expensive option. Many audit firms now provide 'pre-audits' or readiness assessments where they perform the same set of test procedures without issuing an auditor's report. They then repeat the same tests and issue the formal report for an official audit.

Typical items in a pre-audit or readiness assessment may include:

- A policy and procedure review.
- An organizational review.
- A high-level controls architecture review.
- A review of previous audit reports.
- A comparison of a sample group of normal and administrative users' levels of access to what is necessary.
- A review of standard build documents.

- A comparison of a sample of systems with secure build documents.
- A review of change management procedures and selection of a sample of change tickets to review and see if procedures were followed.
- A review of incident-handling procedures and selection of a sample of tickets to review and see if procedures were followed.
- A physical and environmental control walk-through.

By engaging with your auditor before an audit, IT policy design issues became visible and gaps in coverage are identified before the official audit occurs. This extra step increases the cost of an audit program, but it also demonstrates a commitment to compliance. In many cases, the pre-audit consultants can share best practices and show how to adjust focus areas for better balance of resources.

Maintaining auditor/consultant independence and objectivity

Auditors providing consulting services are often subject to sharp scrutiny – especially to whether providing both services impairs objectivity and independence during an official audit. In particular, if a consultant designs and implements controls, he or she may or may not be the appropriate person to attest to the efficacy of those controls. Sarbanes–Oxley, and the standards set by the Public Company Accounting Oversight Board (PCAOB), describes what services an auditor of a public company can provide. By contrast, some industry standards such as the PCI Data Security Standard don't (currently) prohibit the Qualified Security Assessor (QSA) from providing remediation consulting services. To avoid potential conflict, many organizations take the two-firm approach to exhibit transparency. Using separate firms provides the added benefit of an additional set of eyes on your environment.

The bottom line is that your auditor or assessor has certain rules by which it must abide. Your organization can do whatever it needs for audit preparation, but be prepared to spend the additional fees if you use a separate consultant and auditor.

Best Practice #7: Centralize IT Policy Program Management

A business-focused approach to data compliance can be both good and bad. For instance, it is not uncommon for a distributed organization to have its e-commerce line of business be in compliance with the PCI Data Security Standard, while other lines of business have no control framework at all. Ultimately, however, this situation causes the cost of compliance for an enterprise to increase exponentially. In addition, different regions and lines of business that create their own compliance programs can find these programs being incompatible when compliance technologies cannot interact with other technologies vying to paint an enterprise-wide picture of compliance. To be effective, your organization must implement its IT policy compliance program across the whole organization.

Here are some best practices for centralizing IT policy program management in a way that significantly reduces compliance costs:

- Select a common risk model and a set of standards for the organization.
- Normalize reporting so that values are consistent across regions and lines of business.
- Leverage a common set of industry standards such as CIS, AusCERT, ISO, or SANS.
- Validate that policies created by regional teams are accurate and applicable enterprise-wide.

Implementing a risk- and standards-based approach to IT policy compliance has become the norm, for good reason. You may choose from many risk management models, such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), STAR, CCTA Risk Analysis and Management Method (CRAMM), IAM, and Facilitated Risk Analysis Process (FRAP). The key best practice is to standardize on one model across the organization if possible. Be aware, though, that risk models also vary in complexity; some have dozens of risk tiers while others have few. FRAP, for example, is fairly simplistic compared to OCTAVE, but each model has its place in different organizational cultures. Consistency of reporting should be the goal.

A well-defined risk program includes common best practices such as

- Maintaining asset definitions and a process for keeping the inventory up to date, including business layer goals and objectives as part of an asset's valuation.
- Understanding the threat landscape and how probability and consequence of threats are common pairings with vulnerabilities that top the list of remediation tasks.
- Conducting an 'impact analysis' of suggested changes to avoid negative effects of remediation activities on critical business processes.
- Implementing well-defined repeatable processes where a 'rinse-lather-repeat' cycle continuously improves and streamlines processes.
- Collaboration among regional teams to ensure components of the program are standardized and resource requirements are understood for all phases of the program.

Most importantly, you need to set forth all of these best practices in policies and push them consistently to the regions and lines of business.

In addition to a consistent risk model, consider using a standard as guardrails for controls to alleviate the risk. Organizations such as the Center for Internet Security (CIS), Australian Computer Emergency Response Team (AusCERT), International Standards Organization (ISO), and SANS Institute are all proactive and have active user communities that assist in keeping critical issues visible for common technologies. Rather than waste time building policies from scratch, a best practice to adopt is to leverage content provided by these organizations. The CIS, for example, provides usable content in the form of benchmarks for common technologies. CIS content was originally derived from the US National Institute of Standards and Technology's Special Publication 800-53 guidance and Defense Information Systems Agency's Security Technical Implementation Guides (DISA STIG), but they have been very active in providing additional content derived from their user base. AusCERT has also been proactive in security, and its checklist approach can save an administrator significant amounts of time in creating IT security and compliance policies.

How do I know if I have the right policies?

Validation of policies by a platform expert is an often-overlooked strategy that can have disastrous effects without proper implementation.

One organization hired a consultant to build automated controls that met their policy requirements for their Sun (UNIX) systems. The consultant utilized the CIS benchmark tools to create the baseline configuration. Unfortunately, the UNIX administrator who took these policies had simply copied and pasted the same policy to HPUX and the other UNIX flavors. This resulted in numerous audit findings on these other platforms.

From the auditor's perspective, the deployed platforms didn't meet their own control requirements. From the IT manager's perspective, they had consulted several UNIX policies but they lacked the technical expertise to know the difference between applicable controls between UNIX flavors.

As your organization creates and validates policies, be sure to regularly tap the expertise of consultants and product vendors on what they see as the issues and requirements for staying compliant. Never assume you've seen it all. Other people are always out there, willing and able to help.

Generally, leveraging industry-accepted content fosters trust with your IT auditor as opposed to 'home-grown' policies where the auditor must perform significant analysis of documented content. An IT auditor will have a better understanding of a Windows 2003 CIS level I benchmark than a custom Windows policy created by your Active Directory Windows administrator who based the policy on their own expertise. The home-grown policy may be just as applicable, but the auditor must treat the content as an unknown entity and perform a deeper review of the documentation to validate procedures for the audit.

In summary, any technology that you put in place to assist with compliance must

- Reduce or manage your overall risk posture.
- Align your standards-based approach.
- Either support the administrative, physical, and logical controls or integrate with additional data sources that can manage and monitor the controls universe.

Best Practice #8: Prioritize Remediation Activities

Remediation – or the process of fixing deficiencies – is a critical activity. You need to plan and execute it in a manner that is logical, repeatable, and defendable to auditors. Here are some rules of thumb for prioritizing remediation activities:

- Start with the business-critical risks and exposures.
- Address all previous audit findings.
- Look for any instance where one fix can address multiple control weaknesses or findings.
- Go after the low-hanging fruit.

Remediation should leverage a risk-oriented approach based on a solid understanding of business process and the technical environment. Using this strategy, you maximize use of technical resources for securing information assets and improving the business.

Aim to associate the prioritization value of an asset both by its physical cost and by its role in accomplishing a business goal. In this manner, your compliance program can better ensure that you address the most critical deficiencies and exposures that could impact the business first. This process can be time consuming due to dependencies of the business process, so be sure to account for those in planning remedial action.

Repeat audit findings are one of the top reasons why compliance managers are found negligent, and a prime reason why a compliance manager can be relieved of a job. For this reason, reviewing the findings of each audit after that audit has taken place is essential. Addressing discovered lapses, policy violations, and other areas of negligence before the next audit is imperative. Prioritize problem areas for remediation or document them as accepted risks with justification for deviation from policy. When IT auditors next arrive onsite, one of the first things they'll ask for is previous audit documentation.

In many cases, a single technical configuration process or use of a utility can help to remediate multiple issues at once. Group policies on Windows, for example, can help correct

configuration issues in mass. Use of TCP_Wrappers on UNIX can help with hardening multiple network services on UNIX simultaneously. Part of prioritizing remediation is identifying where you get the most 'bang for your buck.' Weighing criticality of the issue is involved, but if a single hour's worth of work can remediate hundreds of issues, good practice is to do it right away.

In prioritizing remediation tasks, a common best practice is to go after the 'low-hanging fruit' – in other words, identify what you can do quickly with greatest impact in order to get momentum rolling in the program. Here are a few examples of fixes to common control weaknesses that fall into the category of 'low-hanging fruit':

- Disabling common prohibited network services like telnet, FTP, TFTP, chargen, and so on.
- Confirming file permissions for common critical files are set as expected.
- Prohibiting software, such as peer-to-peer networking applications, that isn't pertinent to the business.
- Confirming that only authorized individuals have administrator access and require individual account usage where possible for tracking purposes.
- Disabling accounts that haven't been used for a predetermined period.
- Enforcing a minimum password complexity level and audit policies on all systems.
- On Windows platforms, leveraging group policies to confirm security settings are effectively implemented.
- Leveraging security utilities where possible; security tools like TCP_Wrappers and Sudo can greatly help with common compliance issues.

Remediating all deficiencies at once is realistically impossible. Just be sure to document why you didn't close a particular finding either through a risk-based prioritization or a documented exception. Many organizations have exceptions and items that aren't addressed. But when you show your auditor why the risk was low, and that you chose to focus on more critical deficiencies, your position is then more defensible should it be challenged in the next audit.

Best Practice #9: Understand How IT Policy Compliance Management Can Help in Other Areas

Implementing the right IT policy compliance controls can also help you in related areas, such as vulnerability management and change management.

Most IT security staff view IT compliance as an extension of IT security. Surveying the compliance technology landscape confirms this perspective. Providers like Qualys, who started in vulnerability management, saw an opportunity to extend that platform and set of services to support compliance. This support can apply to a specific use case, such as Payment Card Industry (PCI) requirements, or more broadly across multiple regulations and standards. In most cases, configuration compliance requires multifactor vulnerability scanning such that implications can be addressed from a risk and configuration management perspective.

Organizations with good change management capability generally have good policy management, and vice versa. Key challenges for organizations include:

- Keeping change control documentation current.
- Keeping IT asset lists current.
- Managing exceptions and issues.
- Reporting.

A common issue reported by large organizations is keeping up with the IT assets deployed in the environment. Changes are constant: retiring systems, deploying new systems, merging organizations and their assets, and installing new technical releases. Despite this change, many organizations are hit with an audit finding that ties to change management and dependent processes. Planning for this is good practice. Even a minimal investment in asset management capabilities can go a long way.

Automating asset management provides significant benefits for policy compliance. Figure 3-4 is a screen shot from one automated solution – QualysGuard Policy Compliance – which shows point-and-click assignment of IT assets to specific groups. This capability enables instant segmentation for audits of specific policies.

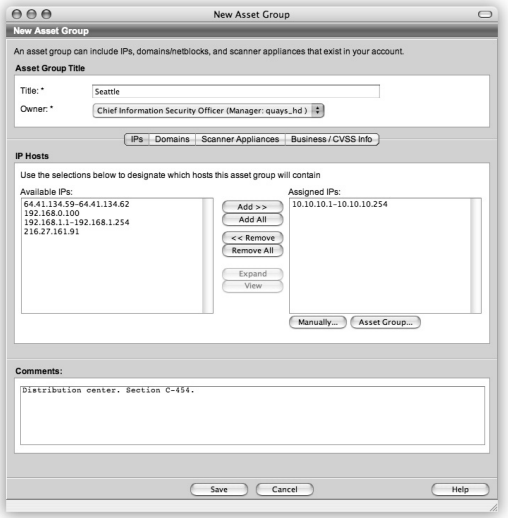


Figure 3-4: Automating IT asset management allows instant segmentation for audits pertaining to specific policies.

In general, exceptions to policies are inversely proportional to the complexity of your organization's policy. Companies that implement a small number of IT policies often must deal with a huge number of exceptions generated during compliance audits. The flipside is that organizations with more detailed policies have to maintain them. Typically however, the cost to maintain is lower than the cost to manage findings during an audit. The old phrase 'pay me now or pay me later' is quite relevant here.

Spotting unused accounts

Many organizations use audit reports to identify user accounts that haven't been used in 'x' number of days. They do this to identify active accounts of former employees who may actually be disgruntled, and who might use those accounts for acts of mischief – or worse. This approach also frees up licenses that the organization can reuse for other employees, saving money.

From a policy compliance perspective, a common standard is that all terminated employee accounts are disabled on day of termination, and deleted no later than 180 days after employment ended. So, leveraging policy compliance data for this purpose also helps from security and cost savings perspectives, and helps to prevent additional data loss. A key best practice is to make sure that an accurate list of systems used by an employee is kept up to date.

IT policy compliance reporting can benefit many areas of an organization's management. For example, IT organizations can use much of the same compliance reporting to identify performance and availability issues so they can increase the quality of service they offer to internal customers.

Many IT operations teams also benefit from automated compliance and security tools to enumerate systems in their environment for categorization. For example, many compliance and security solutions have the ability to audit Windows registry values or UNIX file content, which can subsequently be used to identity machines associated with a particular application or business process. Also, compliance user reports can help manage licenses by identifying active user accounts for employees no longer active in the organization. Those licenses can be reallocated to active employees.

Finally, compliance reporting can identify abuses of authority and confirm that system configuration is consistent across the enterprise. Aligning IT security and compliance with the business is further enabled through data consistent processes and reporting.

Best Practice #10: Regularly Monitor the Whole Compliance Program

We conclude this chapter on best practices by revisiting the concept of the big picture.

The compliance ecosystem

Your *compliance environment* is an ecosystem that includes lots of different components, some IT-related, and some not. Point solutions obviously must fit into an overall policy compliance program, but don't forget that the overall program must receive a sanity check at least annually – and not just when the auditors visit.

Here are some key things to check annually with respect to your policy compliance program:

- Is the overall set of compliance policies being followed?
- Are all of the controls (physical, administrative, and technical) aligned such that you have a comprehensive view of where you stand?
- Are the overall reporting capabilities of point solutions able to be combined for executive level reporting?
- Are data custodians (in other words, IT administrators) able to take the outputs from audits and point solutions and remediate negative control findings?
- Overall, do the combined set of policies, procedures, and technologies drive the appropriate level of accountability across the organization?

Everything comes down to risk

Never forget that your controls must be risk-based, and they must make financial sense. Don't, for example, spend $10 million on controls to protect $5 million in data or potentially $500,000 in fines. Also, don't be afraid to share this context

with your auditors. You have permission to argue your case when needed. Remember, auditors don't typically have the context of what it takes to run your business. Auditors are human and you can reason with them as one professional to another.

"A CISO's perspective"

I am the CISO of a financial Application Service Provider (ASP). A couple years ago, a major audit firm examined my environment. Like most previous audits, the auditors (who appeared to be in their mid-twenties) were here for two weeks, sat in a conference room, and only interacted with my staff when they needed something. Two weeks after they left, I received a qualified report noting several controls flagged as being not in place. Among these, the auditors noted that some of our software developers had access levels that they felt were unnecessarily high for their job levels, router configurations that were not in-line with industry practices, and some general policy deficiencies.

I'd invested the better part of three years building what I thought was a reasonable security program. No security program is perfect, but I felt ours was very strong. As a result, I asked – no, I demanded – that the firm come to my office to meet and discuss the findings. The manager (who wasn't present for the audit) arrived with the 'senior' auditor for my assessment and we walked through the audit findings one-by-one. It became apparent that while the findings appeared correct on the surface, their underlying testing methodology had focused on an area of the business that wasn't a high priority, and thus not a focus for my security team. Furthermore, I pointed out there were likely areas of high value to the business that I was addressing but which the audit team did not consider.

As a result of our session, the auditors returned. Although they didn't change the testing methodology, they did take a broader look at the environment, find some additional items, and deprioritize many of the findings from the previous report. The fact that they'd previously not tested the right controls by taking the broader business into context was frankly not their fault, but mine. I should have been more engaged in what was going on. When a proper audit is based on risk, I couldn't possibly expect a group of young auditors to understand my controls environment without me walking them through why I created it, and how. That's a mistake I'll never make again.

Part IV

Looking at Automation in IT Policy Compliance

In This Part

- Streamlining IT policy compliance with automation
- Surveying solutions for automating IT policy compliance
- Understanding the interaction of compliance technologies and processes
- Measuring cost savings with automated tools

Consistently following the best practices that we outline in Part III means that auditors will generally be satisfied with your IT policy controls. The age-old question is, how do you do all of that without bankrupting your organization?

Considering Automation

With the continuous expansion of IT resources and new technologies such as cloud computing, the in-scope target of systems and networks for auditing continues to grow. For all practical purposes, internal auditors would never be able to review more than a small sampling of user accounts of system configuration settings on a periodic basis. Automation is therefore the only reasonable way to assure that you evaluate an adequate number of systems on a regular basis.

Without automation, you can't be sure that the processes and checks performed by humans are being done correctly and consistently. Obviously, humans are prone to make mistakes. You can verify compliance when its steps are automated and

repeatable, however, and the best way to achieve this is by removing any human subjectivity, bias, or error from the data collection and analysis process. Automation achieves this purpose by applying previously-defined policies and templates across numerous machines.

One important side benefit to automating policy compliance is that the amount of data collected with automated tools can be extremely valuable to auditors, IT administrators, and managers alike. These data can provide important insights to improving operational efficiency. Organizations that use quality control programs such as Six-Sigma regularly deploy automation technologies to measure accuracy, quality, and performance.

Considering Solutions Options for Automating Policy Compliance

A simple Google search reveals hundreds, if not thousands of IT policy compliance technologies, from IT configuration management to Governance, Risk, and Compliance (also known as IT GRC). When considering automation, an organization should consider these questions:

- What control checks are we trying to automate?
- How do we plan to capture the data?
- What changes must we make to our systems to implement the technology?
- What reports do we need to be available internally and externally?

Understanding what automation solutions can do

Many of the products sold to 'make you compliant' end up taking as much time to install, configure, and manage as it would to send a team of auditors to perform the testing manually! However, in its most basic form, this technology should automate tasks that would otherwise be done by an auditor,

thereby reducing the amount of work for people to perform. A common example of this is the collection and analysis of system configuration data, which is then correlated with a set of standard or user-defined policies. This process is generally referred to as 'IT configuration and policy compliance.' Qualys' QualysGuard Policy Compliance is an automated solution within this category.

Figure 4-1 shows the policy compliance lifecycle or workflow that is automated with QualysGuard Policy Compliance.

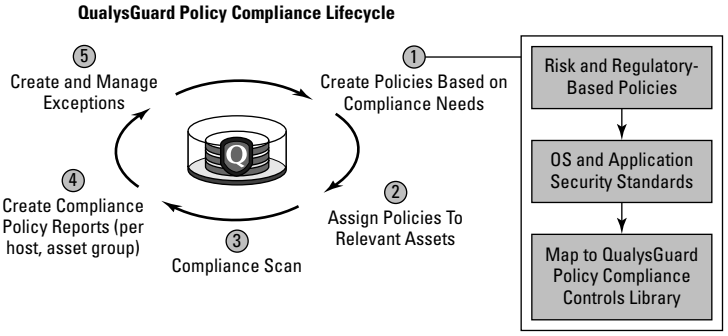


Figure 4-1: Policy compliance lifecycle or workflow automated with QualysGuard Policy Compliance.

To illustrate how these solutions work, consider your Windows-based servers as an example. Whether your policy mandates standards from the National Institute of Standards and Technology or one of several best practices prescribed by Microsoft doesn't matter. There is an expectation that software has been updated with certain patch levels, certain services and default settings are disabled, and strong password policies are enforced, among other things.

Testing this policy requires examining the system registry, account/permission settings, and patch levels. Conducting this exam could easily take an auditor one hour per server. By contrast, an automated policy compliance solution could scan all servers, collect the data, and compare it to policy requirements in just a few minutes.

Given typical access controls, not any user can view this detailed system-level data – and nor should they!

Case study: Large financing company

Industry: Global diversified with financial, manufacturing, energy, and more

Headquarters: Detroit, MI

Locations: Across the US

Employees: 20,000+

'The solution we had in place could not scale to our growing requirements. We spent more time managing agents than in managing our compliance. QualysGuard was easy to use, easy to deploy and allows us to focus on what we do best, which is manage risk.' Global IT Security Manager

Objectives: This large financial services company is under the scope of the Gramm–Leach–Bliley and Sarbanes–Oxley acts, as well as a host of consumer protection laws, and also used an industry-leading agent-based compliance management solution. The company said it was spending 60–80 percent of the time just managing the agent infrastructure for tasks such as agent configuration, uptime, and so on.

Results: Moving to a QualysGuard Software-as-a-Service-based solution, the company quickly saw a drop in time spent managing compliance infrastructure. With that time saving, they could focus more on analysis, reporting, and the workflow associated with pushing findings out for remediation to remote branch offices and data centers.

The Qualys website contains more info and other case studies at `www.qualys.com/customers/success/` for more info and other case studies.

Agent versus agent-less solutions

The market offers you many automated compliance solutions. They usually come in one of two forms: with, or without a software agent:

- *Agent-based solutions* include software installed on each system on which you monitor compliance. These agents then 'phone home' to a management server that collects the information and generates the reports.
- *Agent-less solutions* use scanning technology to connect to the monitoring system, collect the data, and then bring it back to a centralized system for analysis.

The trick is to know which solution is right for you. In general, agent-based solutions work when the IT staff has tight control over desktops and servers, is willing to manage the 'health' or status of the agents, and is also willing to go through the process of agent deployment on each device. With this scenario, extracting the target information is not a simple task. Agent-based solutions see a lot of push back, a common complaint being that running an agent adds additional processing overhead to the machine, which can decrease performance.

Some agent-less solutions also have challenges. Scanning a machine to get audit information requires a high level of access. In large organizations with many domains and administrators, deployment of an agent-less solution can also be challenging – especially without facilitation by automated identity management for access control. The key benefit, however, is eliminating the overhead of an agent. So, as long as you can connect to the machines and you have the prerequisite access, an agent-less solution makes it easier to audit systems, and for auditors and security teams to audit the IT staff.

The QualysGuard Policy Compliance solution takes this agent-less approach one step further. It eliminates the overhead of an agent, and is controlled by users via QualysGuard Software-as-a-Service (SaaS) operating centers. As a result, no agents or additional management software are required.

Flexible Reporting Is a Key Requirement

Reporting is the most valuable capability of an automated IT policy compliance solution. Auditors, security staff, and other users need to be able to access the data and generate reports that meet everyone's needs. This includes people who need the executive 'birds eye' view, as well as technicians who live in the detailed world of granular bits and bytes. The screen shot in Figure 4-2 shows an example of a detailed report – in this case, QualysGuard Policy Compliance providing IT administrators with registry and control setting details that indicate how systems might be misconfigured.

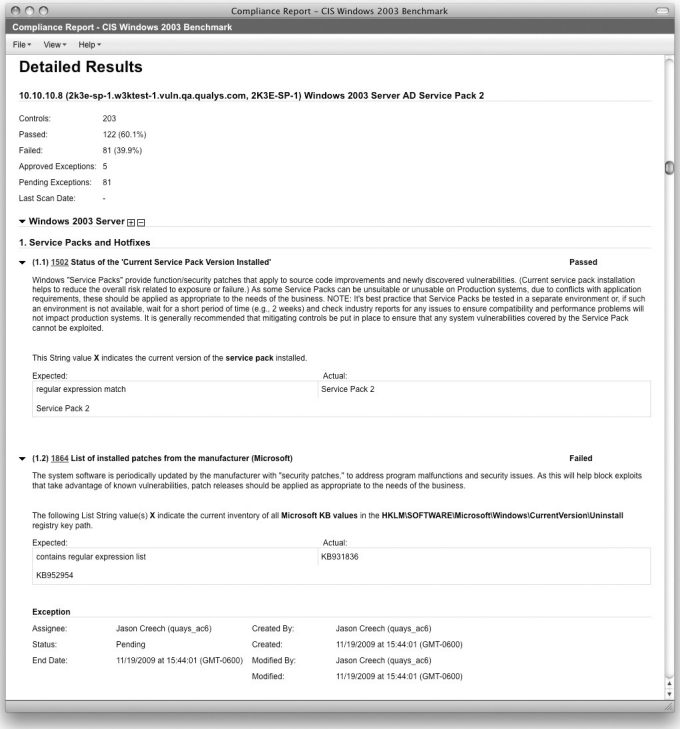


Figure 4-2: QualysGuard reports findings from a Windows Server configuration assessment.

IT policy compliance is a continuous process, so IT managers and Chief Information Officers need to be able to track how in-line systems are working within the established policies. These people are especially keen to review trends via a 'management dashboard.' The screenshot in Figure 4-3 shows examples of higher-level reporting and dashboards provided by QualysGuard Policy Compliance.

It's useful to note that reporting is not a one-size-fits-all science. Every organization requires the capability for customization because there's always someone who wants to look at data not revealed by a canned report. As you check out automated policy compliance solutions, be sure to look for reporting that offers configurable customized options. This capability will enable you to meet requests for unique data with ease.

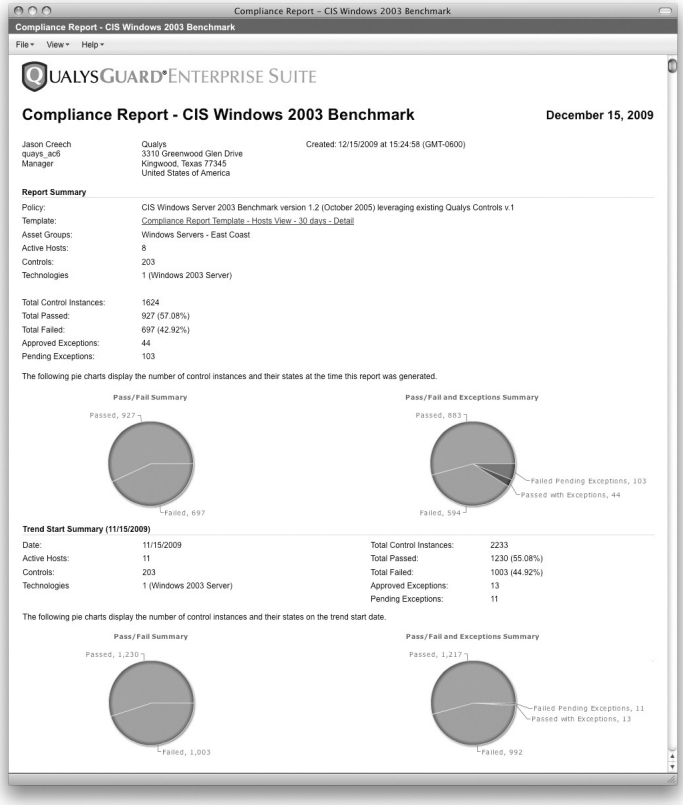


Figure 4-3: QualysGuard Policy Compliance summary findings.

Case study: Fortune 50 Conglomerate

Industry: Global diversified with financial, manufacturing, energy, and more

Headquarters: New York, NY

Locations: Worldwide

Employees: 300,000+

'We have hundreds of thousands of hosts with no conceivable way to ever check them manually. We also have many lines of business covered by many regulations. There was no centralized solution to help us manage our IT Policy Compliance. This is why we turned

(continued)

(continued)

to QualysGuard, which is what we have trusted for years for vulnerability management.' Global IT Security Manager

Objectives: As this large Fortune 50 company grows with frequent acquisitions, the use of simple monitoring tools for compliance was practically impossible. The company needed to apply industry standard controls (NIST) across a wide variety of businesses subject to compliance with a wide variety of laws. Deploying a monitoring agent to its hundreds of thousands of systems was out of the question.

Results: Approximately four years ago, this company partnered with Qualys to leverage its vulnerability management to scan its vast networks. Qualys worked closely with the company to fine-tune operational processes and reporting.

With its existing base of Qualys scanners and Software-as-a-Service architecture, adding policy compliance to the vulnerability management solution took a small fraction of the effort that it would have done to deploy another solution.

On an ongoing basis, the company's compliance and risk management teams can now focus on analysis and improvement strategies versus the day-to-day operation of auditing hundreds of thousands of hosts.

See `www.qualys.com/customers/success/` for more info and other case studies.

Looking for Interactivity with Other Systems

Auditors and security administrators often need to share and correlate IT compliance data with other information. For example, IT configuration data is often reviewed in conjunction with a security incident. This forensic analysis helps to determine the root cause of a policy violation. From a broader compliance perspective, IT configuration data is regularly added to non-technical (or softer) compliance sources such as policies, procedures, and the results of manual audits. All of this relates to Governance, Risk and Compliance, more of which is described in the sidebar of the same name.

Governance, risk, and compliance

Governance, risk, and compliance (GRC) technologies spawned from a need in the early 2000s for companies to centralize audit data collected for Sarbanes–Oxley compliance. Early adopters, such as Paisley and Open Pages, were companies started by ex-Big Four auditors looking to help centralize the audit data collection process. The industry now includes broader compliance use-cases such as vendor management, policy enforcement, and change management. Currently, the market is still somewhat fragmented, with niche players such as Modulo (`www.modulo.com`), the latter recently acquired by EMC, and Archer (`www.archer.com`) offering a more comprehensive and modular solution. Non-traditional GRC technology providers are also beginning to add certain elements of workflow and reporting that have made solutions like Archer popular among some users.

The automated policy compliance solution you choose should include capabilities such as open Application Programming Interfaces (APIs) that enable it to send data to another application. The reality is that for every interoperability or integration use case, there are five other use cases that have yet to be revealed – hence the unequivocal need for flexibility in an automation solution.

Knowing that Automation Is All About Cost Savings

The final choice of an automated IT policy compliance solution often comes down to cost. With a manual solution and infinite resources, you could task 100 auditors with reviewing the configurations of all the systems in your environment. By adding even more resources and processes, you could probably make the results consistent. The total price tag for doing all of that manually would range from six to seven figures – each time you wanted to assess policy compliance! IT policy compliance automation allows you get more coverage and more precision for less money.

Successful choice and deployment of an automated IT policy compliance solution requires that you:

- **Understand your risk profile and scope.** How often do you need to assess your organization's systems and what level of scope (or sample size) are you comfortable in using for assessment?
- **Do your homework on available solutions.** In general, an acceptable cost equation is:

  Cost of Technology + (Cost of People 'Setup' + Cost of People 'Ongoing') < Cost of Manual Internal Audits
- **Prepare for implementation.** You need to devise policies and standards for measuring results.
- **Use it!** Unless you have a formal process for reviewing the data and responding to negative findings, the investment will have no value. Be sure to constantly reassess how you use the technology to determine if the underlying processes for audit and use of the technology are optimal for your organization.

Part V

Ten Tips for IT Policy Compliance

In This Part

- Understanding the main points of IT policy compliance
- Following steps to implement controls and processes for policy compliance
- Improving IT policy compliance with automation

For most organizations, IT policy compliance is a big fact of life. The tips in this part can serve as a handy checklist to help you prepare for compliance and the auditors who work hard to find things your organization forgot to do. Determine what you must do for IT policy compliance and stick with the process, so that you can proceed with confidence!

Read This Book

If you're reading this part first, consider that (in our humble opinion) there's no quicker way for an organization to get the gist of IT policy compliance than to read the whole of *IT Policy Compliance For Dummies*. This book describes what it is, how to prepare, and how to tap the benefits of automation in the ongoing process of IT policy compliance. Start between these covers – you won't be sorry!

Understand the Importance of IT in Policy Compliance

Compliance is about conformity with accepted standards. Usually, this means obeying laws and regulations that apply to your business. Information technology is so important in policy compliance because of the crucial part it plays in the operation of modern businesses, and compliance often relates to the way your organization uses IT.

Information technology compliance is the implementation and management of IT in accordance with accepted standards. This includes technical standards, and how people use that technology in the course of business operations.

Determine the Relevant Laws and Regulations

Laws and *regulations* articulate the 'policies' governing their requirements. Examples include the Sarbanes–Oxley Act (SOX) to regulate financial reporting, the Gramm–Leach–Bliley Act (GLBA) to regulate non-public personal information (including financial data), the Health Insurance Portability and Accountability Act (HIPAA) to regulate protected health information processed by health care organizations, and many others. You can't begin the process of policy compliance without knowing which laws and regulations apply to your company.

Ascertain What Controls Apply to the Laws and Regulations

Controls are the technical and process-oriented means to comply with policy. Controls are specified by various government and industry standards, such as Control Objectives

for Information and Related IT (COBIT), National Institute of Standards and Technology (NIST), International Standards Organization (ISO), and the Payment Card Industry Data Security Standard (PCI DSS). As with laws and regulations, compliance requires that you determine which controls apply to your organization. Auditors rely heavily on these controls, which are standard procedures for IT policy compliance.

Align IT Policy Compliance and Security with the Business

Aligning compliance with business entails understanding your organization's culture. Is it highly process-driven, or does it have more of an ad-hoc, chaotic way of doing things? If it's the former, issuing detailed policies may be adequate for ensuring compliance. But if it's the latter case (a common situation!), you need controls that are preventative and detective in nature. Your controls should address the specific business risks related to policy.

Executives buy in more when you can speak their language of business. Doing this also helps auditors to understand the reasons why your organization deployed particular controls, or perhaps decided to accept certain levels of risk.

Understand Your IT Environment

Your IT environment directly affects the design of your policy compliance program. The two common types of environments are:

- A *homogeneous environment,* which is largely consistent, with IT deployments consisting of standardized vendors, models, and configurations.
- A *heterogeneous environment,* which uses a broad range of technologies, versions, and even different compliance and security applications.

In general, the cost of compliance is less expensive for homogenous environments. Fewer technology types, fewer technology vendors, and fewer technology versions translate to fewer policies and less complexity. This results in a lower cost of compliance and security per system because individual processes impact greater percentages of the IT volume.

Take extra care to ensure policies adequately address new technologies, such as cloud computing and virtualization. Cloud computing, in particular, requires policies with a higher emphasis on administrative controls and slightly less on technical security controls, because you're delegating management of the hosting and network systems.

Establish Accountability

IT policy compliance programs don't work without accountability. *Accountability* involves the definition of organizational roles and responsibilities – which set out what assets an individual is responsible for protecting and who has authority to make decisions.

Accountability starts at the top with executives; you stand a better chance of their active involvement by casting IT policy compliance in terms of business risks rather than technology. As for the IT department, they have two main roles:

- As *data/system owners*. The owner is a member of the management team who is responsible for how data is used and its ultimate care, and is accountable for managing and protecting the information.
- As *data/system custodians*. Specific custodial roles may include system administrator, security analyst, internal audit, legal counsel, and so on.

Policies are especially important for these roles. Auditors carefully verify the execution of compliance activity in conjunction with authorized roles and designated accountability.

Prioritize Remediation of Vulnerabilities and Audit Issues

Remediation is a critical activity that must be planned and executed in a manner that is logical, repeatable, and defendable to auditors. Start with the business-critical risks and exposures; address all previous audit findings; look for any instance where one fix can address multiple control weaknesses or findings; and go after the low-hanging fruit first!

Remediation should leverage a risk-oriented approach based on a solid understanding of business process and the technical environment. Aim to associate the prioritization value of an asset by its physical cost and by its role in accomplishing a business goal. By doing so, your compliance program can better ensure that the most critical deficiencies and exposures that could impact the business are addressed first.

Use Automation for IT Policy Compliance

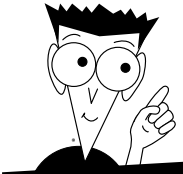
Your IT assets are continuously evolving and growing in number. For internal auditors to review more than a small sampling of user accounts or system configuration settings on a periodic basis is practically impossible. Automation is the only reasonable way to assure that you evaluate an adequate number of systems on a regular basis.

Automation enables auditors to verify compliance better because it automates the testing of all steps and all controls – without human subjectivity, bias, or error from the data collection and analysis. Automation does this by applying previously-defined policies and templates across numerous machines. It also reduces the number of people that you need to assign to the process, saving money, and speeds analysis with instant reporting, which accelerates spotting and remediating issues. Data collected by automated IT policy

compliance can also help an organization improve business processes. IT policy compliance automation with a solution like QualysGuard Policy Compliance enables your organization to get more coverage and more precision for less money.

Monitor Your IT Policy Compliance Program Regularly

We conclude this chapter and book by re-stating the Big Picture: Regularly check the "sanity" of your IT policy compliance program to make sure that controls are appropriate and risk based. They must make financial sense to the business. Establish your justifications before auditors arrive, and don't be afraid to share the business context with them should questions arise about a particular control. The presence of your automated IT policy compliance controls with well-reasoned business context for each one will help ensure that your company passes the audit – and viably enforce IT policy compliance throughout the organization.

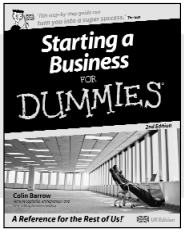


FOR DUMMIES®

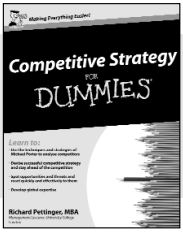
Making Everything Easier!™

UK editions

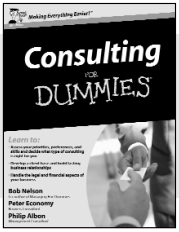
BUSINESS



978-0-470-51806-9



978-0-470-77930-9



978-0-470-71382-2

Body Language For Dummies
978-0-470-51291-3

British Sign Language For Dummies
978-0-470-69477-0

Business NLP For Dummies
978-0-470-69757-3

Cricket For Dummies
978-0-470-03454-5

Digital Marketing For Dummies
978-0-470-05793-3

Divorce For Dummies, 2nd Edition
978-0-470-74128-3

eBay.co.uk Business All-in-One For Dummies
978-0-470-72125-4

English Grammar For Dummies
978-0-470-05752-0

Fertility & Infertility For Dummies
978-0-470-05750-6

Flirting For Dummies
978-0-470-74259-4

Golf For Dummies
978-0-470-01811-8

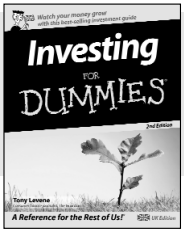
Green Living For Dummies
978-0-470-06038-4

Hypnotherapy For Dummies
978-0-470-01930-6

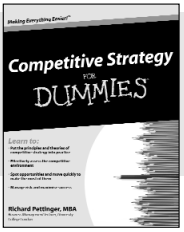
Inventing For Dummies
978-0-470-51996-7

Lean Six Sigma For Dummies
978-0-470-75626-3

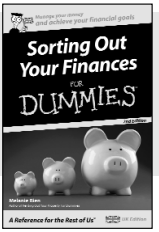
FINANCE



978-0-470-99280-7

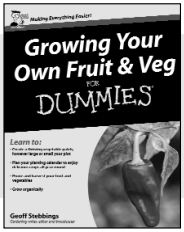


978-0-470-77930-9

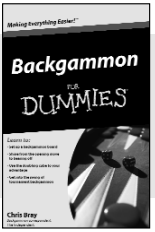


978-0-470-69515-9

HOBBIES



978-0-470-69960-7



978-0-470-77085-6

978-0-470-75857-1

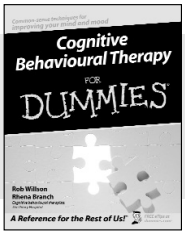
Available wherever books are sold. For more information or to order direct go to www.wiley.com or call +44 (0) 1243 843291

FOR DUMMIES®

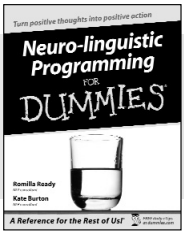
A world of resources to help you grow

UK editions

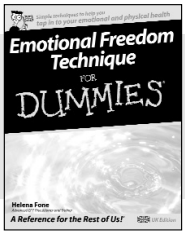
SELF-HELP



978-0-470-01838-5

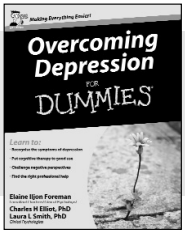


978-0-7645-7028-5

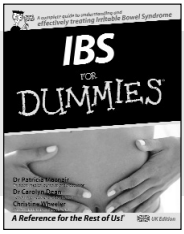


978-0-470-75876-2

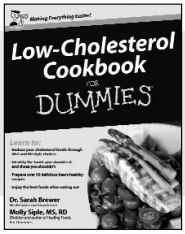
HEALTH



978-0-470-69430-5

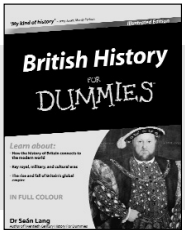


978-0-470-51737-6

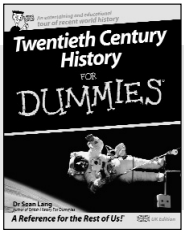


978-0-470-71401-0

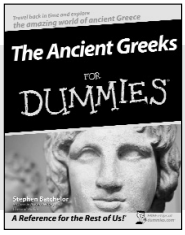
HISTORY



978-0-470-99468-9



978-0-470-51015-5



978-0-470-98787-2

Motivation For Dummies
978-0-470-76035-2

Personal Development All-In-One For Dummies
978-0-470-51501-3

PRINCE2 For Dummies
978-0-470-51919-6

Psychometric Tests For Dummies
978-0-470-75366-8

Raising Happy Children For Dummies
978-0-470-05978-4

Reading the Financial Pages For Dummies
978-0-470-71432-4

Sage 50 Accounts For Dummies
978-0-470-71558-1

Study Skills For Dummies
978-0-470-74047-7

Succeeding at Assessment Centres For Dummies
978-0-470-72101-8

Sudoku For Dummies
978-0-470-01892-7

Teaching Skills For Dummies
978-0-470-74084-2

Time Management For Dummies
978-0-470-77765-7

Understanding and Paying Less Property Tax For Dummies
978-0-470-75872-4

Work-Life Balance For Dummies
978-0-470-71380-8

Available wherever books are sold. For more information or to order direct go to www.wiley.com or call +44 (0) 1243 843291

06439_p2

Qualys: The Leader of On-Demand Security and Compliance Management

Qualys is the leading provider of on-demand IT security risk and compliance management solutions – delivered as a service. Qualys solutions perform more than 250 million IP audits per year, and are the widest-deployed security on demand solutions in the world. Among these is QualysGuard Policy Compliance, which automates the collection of OS Configuration and Application Access controls from information assets within the enterprise. Automated reporting leverages a comprehensive knowledge base of technical controls mapped to prevalent security regulations, industry standards, and compliance frameworks. Auditors use this documentation to verify how an organization provides security and integrity, prove that policies have been effectively operationalized, and verify that the organization has discovered and addressed any policy compliance issues, either through direct mitigation or justification of risk acceptance.

QualysGuard Awards

QualysGuard is overwhelmingly recognized as the leader in its space. QualysGuard has won awards ranging from Best Vulnerability Management Solution, Best Security Product, Best Security Company, Best Network Protection Service and much more!

IT policy compliance needn't be scary!

Implement a successful IT policy compliance program within your company

This book is a quick guide to understanding IT policy compliance. It surveys the best steps for preparing your organization's IT operations to comply with laws and regulations — and how to prove compliance to an auditor. This book also tells you about the leading solution for automating IT policy compliance — QualysGuard Policy Compliance. An electronic version of this book is available at www.qualys.com/itpcfordummies.

Discover:

- *What IT policy compliance is all about*
- *How laws and regulations govern compliance*
- *Ten best practices*
- *How automation can ease compliance and save money*

THE DUMMIES WAY®

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

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*

ISBN: 978-0-470-66535-0
Not resaleable

For Dummies®
A Branded Imprint of
WILEY