



## **Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs**

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **Introduction**

The emergence of new laws and regulations in recent years means that information security has rapidly evolved from mainly a technical problem into a business challenge, grabbing the attention of executives in companies across the globe. These new regulations are forcing companies to adapt their IT operations to the newer security provisions, demonstrating proof of security across their complex IT infrastructures and ensuring that employees and partners understand and abide by the policies. Corporate concerns about achieving compliance are fueling a host of information security initiatives that often involve consultants as well as internal and external auditors. As a result, most companies face an urgent need to implement IT controls that help them demonstrate compliance while improving the protection of their information assets.

According to industry analysts, security incidents, security audits and new regulations are the primary drivers influencing this evolution in information security. In the past, these drivers were considered as separate and distinct IT challenges, most effectively addressed by separate solutions. Today, business executives and industry analysts acknowledge that these drivers are interconnected and that it is now imperative that organizations resolve them through a more holistic and integrated approach.

### **Rapid Acceleration of Incidents and Threats**

Security breaches are a major business risk. Virtually every business now networks its employees, connecting its global systems to the Internet and establishing an IT infrastructure to electronically transact business with partners and customers. The need to secure these information assets and interconnected infrastructures has become one of the most important and widely recognized IT responsibilities in recent years.

### **Costly External and Internal Audits**

A recent Computer Security Institute/FBI Annual Computer Crime and Security Survey [1] indicates that more than 80 percent of its respondents conduct security audits. Two primary factors contribute to the need for more thorough security audits. First, the regulatory environment mandates audits for compliance with standards to demonstrate due care as well as adherence to stated security policies. Second, the exponential increase in Internet communications has also increased audit requirements designed to protect and assure the privacy of personal information.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **Urgent Need to Comply with Regulations**

The need to comply with multiple regulations has increased as legislation such as Sarbanes-Oxley, HIPAA, and GLBA have taken effect. This urgent need has led to a dramatic rise in compliance spending. For example, companies in the U.S. will spend nearly \$15.5 billion on compliance-related activities this year according to AMR Research [2], with the total tab for compliance estimated at \$80 billion over the next five years. Spending on Sarbanes-Oxley alone will exceed \$6 billion in 2005 according to AMR. Of this amount, \$2.6 billion goes to pay for internal personnel devoted to compliance, while another \$1.7 billion is being spent on consultants and external auditing firms.

### **Overwhelming Challenge**

The primary responsibilities of security executives and managers have become overwhelming. They are responsible for securing multiple technologies within a complex, heterogeneous and often global environment. These technologies are constantly changing, and new technologies are constantly emerging. Further, they need to build security policies and make sure that the policies are understood and followed by employees and contractors. Most recently, they need to understand the regulations that apply to their business and make sure that their company can demonstrate compliance. They have to perform these and other responsibilities with limited staff resources and budget.

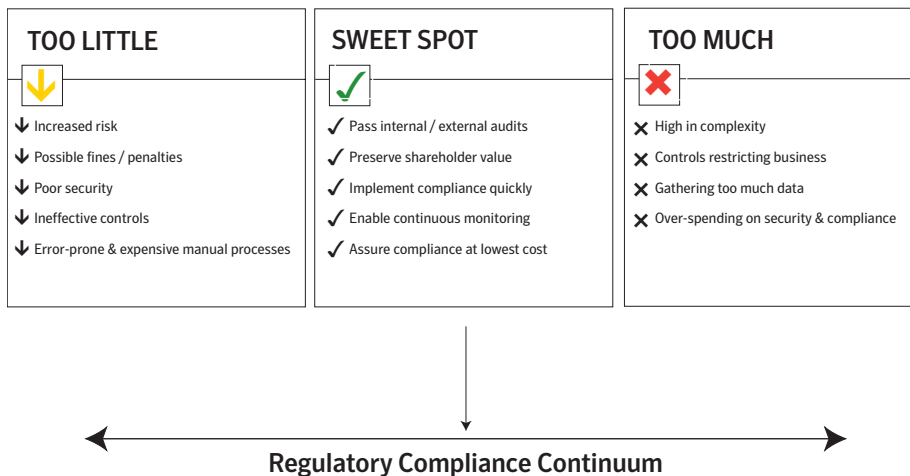
Security executives face an ever-expanding number of critical demands, yet they work in an environment where failure is not an option. If a company experiences a security breach, for example, significant damages may occur on many levels, including the loss of investor and customer confidence. If a company fails a regulatory audit, the executives may be subject to criminal and civil penalties.

These pressures can cause considerable stress and strain on IT operations. According to one security professional in a recent *InfoWorld* article [3], "We literally stopped all other projects for over three months while we documented every security and auditing process we had in place." This was in response to an internal audit aimed at demonstrating compliance.

# Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

## Hitting the Compliance "Sweet Spot"

Judging how much security is enough and then demonstrating compliance by passing audits has become one of the biggest challenges for most organizations. If a regulation requires auditing, how much auditing is enough? The dilemma faced by organizations can, in part, be expressed in Figure 1. The diagram illustrates a security and compliance continuum, with a desired "sweet spot" organizations want to find in order to optimize their time and effort spent on compliance.



**Figure 1 - The Goal: Find your organization's compliance "sweet spot"**

While complying with regulations is one of the top issues facing businesses today, many IT security executives are confused about what specifically they must do to achieve compliance. As a result, they can easily allocate either too much or too little staff time, money and outside consulting resources pursuing a seemingly elusive goal.

# Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

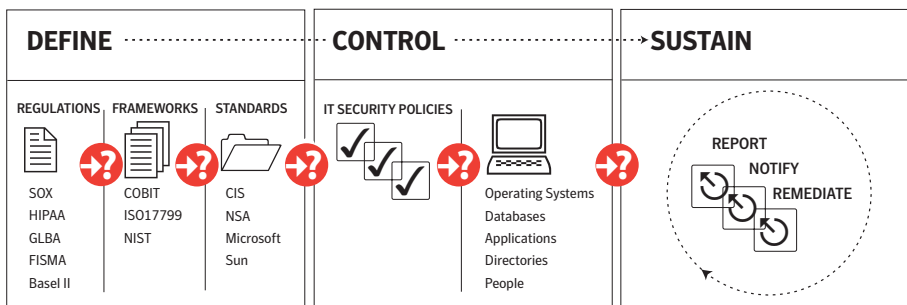
## The Compliance Process Challenge

Improving security and demonstrating compliance for most companies is extremely difficult and expensive to achieve due to the complexity, scope and knowledge required to solve the problem. Figure 2 illustrates the key technical and business challenges that compliance and security professionals face in cost-effectively improving security, while at the same time demonstrating regulatory compliance.

*The compliance challenge can be organized according to three stages:*

1. Define regulations, frameworks and standards that apply to your organization.
2. Implement standards to support policies and apply specific IT technical controls to achieve compliance.
3. Demonstrate due care and sustain compliance by showing that IT controls are in effect and are working properly.

### SECURITY COMPLIANCE LIFECYCLE



**Figure 2 - Compliance Challenges**

Because regulations do not provide specific guidance, organizations must translate regulations into frameworks and standards that can be mapped to specific IT control policies across the enterprise. Once established, these controls must then be sustained on a continual basis to help assure compliance and remediate deficiencies.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **You Are On Your Own**

Organizations have typically been left on their own to develop the appropriate controls for their particular company and industry, especially when it comes to demonstrating how controls operate to satisfy audits. Once established, IT controls and security require continuous monitoring, with prompt response and remediation of violations and deficiencies. In addition, very few companies have the critical mass of regulatory and security expertise necessary for integrating compliance into the business—rapidly or efficiently. Yet, they are being asked to satisfy audits and achieve compliance, with stiff penalties as the consequence of failure.

*Achieving IT security compliance today is difficult for several reasons, requiring security and compliance professionals to:*

- Identify, understand and interpret the regulations that apply to their business
- Translate those regulations into a generally accepted best practices framework, which provides the structure used to define operational policies and technical controls
- Map best practice frameworks into sets of technical controls and operational policies
- Integrate technical controls and operational policies across their IT infrastructure and their people
- Document and continuously monitor their compliance status, and demonstrate proof of compliance to auditors, executive management and other stakeholders.

### **Stage 1: Define Security Compliance—No Easy Task**

While the process appears simple, regulations are not specific when it comes to the exact IT controls necessary to satisfy compliance. Regulations are constantly evolving and can therefore be interpreted differently by different companies. Yet these regulations must be translated into specific IT controls, documented and then enforced consistently throughout the organization's technical infrastructure and among its people.

"Most organizations are baffled when it comes to compliance," according to Paul Proctor, a META Group analyst [4]. With little concrete guidance, many companies are scrambling to assure that IT security and other processes meet regulatory requirements as time runs out and grace period extensions expire.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

One of the most difficult challenges for organizations is to translate the general statements of laws and regulations into specific and defensible controls for compliance. There is no simple, clear definition or consensus as to what encompasses compliance, and no distinct roadmap for how to achieve compliance.

Many analysts have suggested that to establish compliance, organizations should follow a recognized control framework. These frameworks include COSO, NIST and COBIT. The adoption of an IT controls framework, for example, can provide a high-level structure for implementing controls and supporting validation of controls with regulators and auditors.

While these frameworks provide the structure used to help define operational policy and technical controls, they do not provide sufficient detail to enable the implementation of specific controls and policies.

Standards, such as the Center for Internet Security benchmarks [5], provide a more detailed and specific set of generally accepted controls for the configuration of servers, for example. A properly defined compliance structure will map regulatory requirements to a framework such as COBIT. The framework will then guide the creation of operational policies, along with specific, detailed technical controls.

Once this extensive and complicated interpretation and mapping is achieved, the challenge shifts to implementing IT controls based on specific policies.

### **Stage 2: Implement IT Controls Based on Specific Policies**

From an IT security perspective, the key to compliance is in the documentation, monitoring and management of a compliance control structure for your specific enterprise environment. This compliance control structure consists of operational policies and technical controls that are aligned to your business risks and regulatory requirements. Documentation of this structure has become a priority for auditors. As a recent article in *InfoWorld* magazine noted [3], "Auditors aren't simply going to ask you whether or not you've got controls anymore. They're going to want to see documentary evidence to that effect and in many instances will want to come on-site to test them."

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

Your compliance control structure establishes accountability, responsibility and risk management principles that ultimately are mapped to specific controls on individual components of your infrastructure.

- Operational policy controls consist of written statements of expected behavior for individuals and the operational processes they must follow. These controls include, for example, security incident response procedures.
- Technical controls include policies and controls that can be technically automated or enforced across the IT infrastructure. Technical controls, for example, would include a company's password policies, as well as the secure configuration and protection of system servers.

### **Stage 3: Demonstrate and Sustain Compliance**

Once a compliance control structure is established and operational procedures and policies are documented, the compliance burden shifts to continuous IT infrastructure assessment, validation and monitoring. Regulators and auditors want to be assured that when gaps in a control structure become evident, the organization promptly identifies remediation tasks and completes them. Auditors also provide an independent analysis of gaps in the management of compliance architecture and associated programs. Organizations must therefore be able to automate processes that assure the ability to sustain compliance through continuous monitoring, reporting and remediation.

#### ***The Solution: Simplify, Automate and Reduce the Cost of Demonstrating Compliance***

Improving security and demonstrating compliance is extremely difficult to achieve due to the complexity, scope and knowledge required to solve the problem. It is therefore imperative that security software products maximize their value to your enterprise by helping you improve the security of your IT environment and demonstrate compliance. Due diligence in security must translate into due care for compliance.

Glossary of Compliance Terms:

*Policy:* A generalized requirement or business rule that is specific to an organization and represents management's guidance to workers who are tasked with the day-to-day decision-making of operating the organization. Policies typically include general statements of goals, objectives, beliefs, ethics, controls, and worker responsibilities.

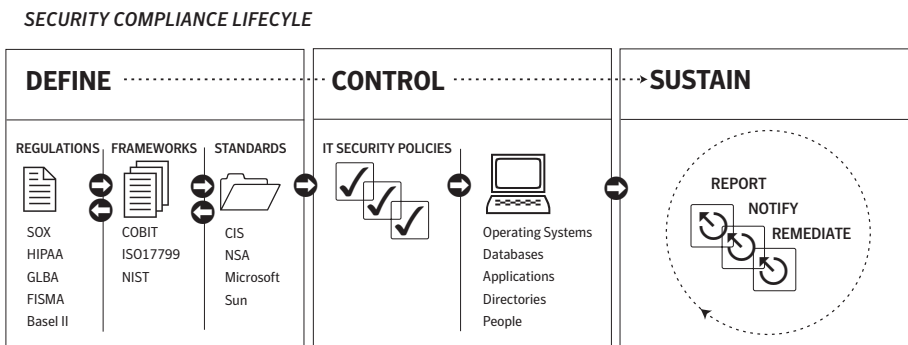
*Regulation:* A regulation that is issued by a regulatory entity or as a result of government legislation. Regulations contain rules that are imposed on organizations and typically have requirements that must be met to avoid fines, loss of access to markets or accreditation. Regulations typically refer to frameworks and standards for practical application and demonstration of compliance.

*Framework:* A methodology of performing an evaluation typically created by an industry leader or a consortium of auditing entities. Frameworks are the prescribed method to evaluate compliance. A framework may also include standards and recommended policies as well as the method for implementing, documenting and testing standards.

*Standard:* A common set of checks, rules or methods that have been created by an industry leader or consortium to provide consistency. Standards are adopted by organizations as being generally acceptable best practices. For example, the Center for Internet Security will issue security checks that can be applied in an organization as "security best practices."

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

Unlike any other vendor, Symantec offers proven, practical IT security compliance solutions that remove the barriers limiting your ability to cost-effectively demonstrate and continuously monitor compliance. The Symantec Compliance Solution is illustrated in Figure 3.



**Figure 3 - The Symantec Approach to Compliance Solutions**

Effective compliance solutions must leverage framework and technical standards to implement IT controls that incorporate specific policies, secure configurations and proper user access. Organizations must then be able to continually demonstrate evidence of compliance through regular documentation and reports.

Symantec Helps You Resolve These Compliance Challenges:

- Do you struggle to understand and interpret regulations and how to apply them?
- Are you seeking to effectively map industry frameworks to technical standards and policies that can be practically implemented?
- Are you frustrated trying to integrate best practices into your complex, heterogeneous IT environment?
- Would you like to deliver reports that clearly demonstrate compliance to auditors?
- Do you wish you could continually monitor your compliance posture and remediate issues as they occur?
- Are you spending far too much in resources and time trying to demonstrate compliance to stakeholders?
- Are you wondering how you'll demonstrate compliance for the next round of audits, once you get past your first compliance audit?
- Do you lack the staff expertise to manage the responsibility of compliance?

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **Symantec IT security compliance solutions enable you to demonstrate compliance across your enterprise at the lowest possible cost by helping you:**

- Define compliance through frameworks and standards mapped to regulations
  - Symantec understands regulations and how they apply to your business, supported by expertise from our professional services and RAZOR teams.
  - Symantec translates regulations into generally accepted frameworks and standards that provide the structure used to define operational policies and technical controls.
  - Symantec maps industry-accepted frameworks and standards to a set of technical controls and policies.
  - Symantec's software incorporates generally accepted best practice frameworks and standards, enabling you to leverage the same information used by your auditors when they validate compliance.
- Implement compliance policies and IT controls based on accepted standards
  - Symantec provides specific configuration settings mapped to IT policies that enable you to implement controls across your heterogeneous IT infrastructure.
  - Symantec provides the flexibility to customize operational policies and technical controls, including exceptions, to meet your specific needs.
  - Symantec provides tools to help you secure acknowledgment and agreement of personnel to security policies.
- Demonstrate due care and sustain compliance
  - Symantec automates procedures to help you continuously monitor and report on your compliance posture, enabling you to demonstrate compliance in a fraction of the time compared with manual methods.
  - Symantec provides regulatory report views that document and help you demonstrate compliance.
  - Symantec provides recommendations for remediating risks or holes in your security posture.
  - Symantec integrates with leading help desk and operational monitoring solutions such as Remedy®, HP® Service Desk, and HP® OpenView® so that you can leverage existing technology.
  - The Symantec support and professional services team offers a full complement of services enabling you to leverage our compliance expertise and ensure success in your organization.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### Compliance Made More Cost-Effective with Symantec

Much of the time and effort spent on implementing compliance in an organization does not directly involve IT-related tasks. Interdisciplinary teams, and often consultants, typically must scope the compliance project, review existing policies and processes and evaluate them across various functional areas and departments.

The table shown in Figure 4 illustrates a comparison of staff-days spent on both non- IT-related and IT-related tasks involved in achieving and sustaining compliance. The numbers are based on a report published by IDC.

#### IT AND NON-IT RELATED COMPLIANCE TASKS

TYPE	TASKS	FREQUENCY / YEAR	COST	TOTAL COST / YEAR
NON-IT-RELATED	Create compliance scope of work	1	10	10
	Establish/review policy	1	10	10
	Project management	1	20	20
	Design/Review sales processes controls	1	10	10
	Design/Review revenue recognition controls	1	10	10
	Design/Review SOD controls	1	10	10
	Design/Review reporting process controls	1	10	10
	Design/Review business process controls	1	10	10
	Design/Review purchasing inventory controls	1	5	5
	Design/Review other systems controls	1	15	15
	Design/Review HR process controls	1	5	5
	Implement/update controls	4	15	60
	Test controls	4	10	40
	Evaluate material weaknesses	4	10	40
Submit exemptions	4	10	40	
<b>NON-IT-RELATED TOTAL STAFF-DAYS</b>				<b>295</b>
IT-RELATED	Design/Review IT controls	4	10	40
	Run IT controls	52	10	520
	Disseminate to stakeholders	52	2	104
	Remediation	52	5	260
	<b>IT-RELATED TOTAL STAFF-DAYS</b>			

**Figure 4 - Comparison of IT and Non-IT-related compliance tasks**

Most organizations spend far more time and effort on IT-related tasks when implementing and sustaining compliance.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

When you add the number of IT-related tasks in implementing compliance, they account for only about 1 in 5, or 20 percent of all tasks. But when you compare the staff-days required to accomplish IT tasks versus non-IT tasks, the vast majority of time involved in compliance (85 percent) is spent on IT-related tasks such as evaluating and running IT controls and remediating problems or gaps.

Thus, IT-related compliance tasks represent the most significant expense in time and money for most organizations. One reason for this is that, unlike non-IT-related tasks, IT-related tasks are not one-time events. In many cases, IT-related compliance tasks must occur on a weekly or even daily basis, while non-IT-related tasks might happen only once or twice a year.

***Industry analysts generally agree that IT security and control technologies can help simplify and reduce the cost of demonstrating regulatory compliance by automating critical functions that include:***

- Policy management to define and enforce both technical controls for the IT infrastructure as well as behavioral guidelines for personnel.
- Configuration management to define how IT resources must be configured to make them secure.
- Vulnerability management to discover and mitigate vulnerabilities and lapses in security policies.
- Identity and access management controls to assure appropriate access to IT resources and applications.

These are precisely the areas that Symantec solutions address with products that have proven themselves with more than 5,000 customers worldwide over the past 15 years. The diagram shown in Figure 5 illustrates the solution categories that Symantec products address in order to automate key functions, improve accuracy and security, and reduce costs.

Time Is Money: Symantec Saves You Both

Recognizing that the vast majority of time spent on implementing and sustaining compliance involves IT-related tasks, IDC states in a recent white paper: "IDC believes a technology solution providing both the security required by the regulations, and a way to translate the nebulous regulations into actionable policy and technical controls would greatly save time thereby saving money."

In its own comparison of achieving compliance through outside consulting services, internal manual procedures, and internal automated procedures, IDC concluded: "Over a three year period, Symantec's software solution can cost up to 90% less than outsourcing, and half [50%] of a manual process handled internally."

IDC explained that, "The reason for the cost savings is because software solutions, such as Symantec's, are squarely aimed at the most labor intensive and complex IT controls related to compliance challenges that organizations must tackle, like maintaining secure and consistent configurations across complex heterogeneous environments based on a broad array of regulations, frameworks, and standards."

Source: "Reducing the cost of compliance," Charles Kolodgy, Christain Christiansen, *IDC Opinion*, June 2005.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs



**Figure 5 - Symantec IT security compliance solutions**

Symantec provides Policy & Compliance Management, Vulnerability & Configuration Management, and Directory & Access Management software solutions that combine best-practices knowledge with automated controls to help you demonstrate and sustain compliance at reduced cost.

**Policy & Compliance Management:** Symantec provides the best, most practical and cost-effective solutions to help organizations manage policies and demonstrate compliance with new and evolving regulations. Symantec's extensive experience and built-in knowledge makes it possible for companies to translate the generalities of regulations into specific IT security controls that can be documented and enforced.

**Vulnerability & Configuration Management:** Symantec helps organizations assess vulnerabilities, secure configurations and remediate exposures for servers, workstations, users, applications and networks. Through a combination of automation, reporting and scheduling options, Symantec solutions help assess and remediate IT risk from both internal and external factors across large, multi-platform environments.

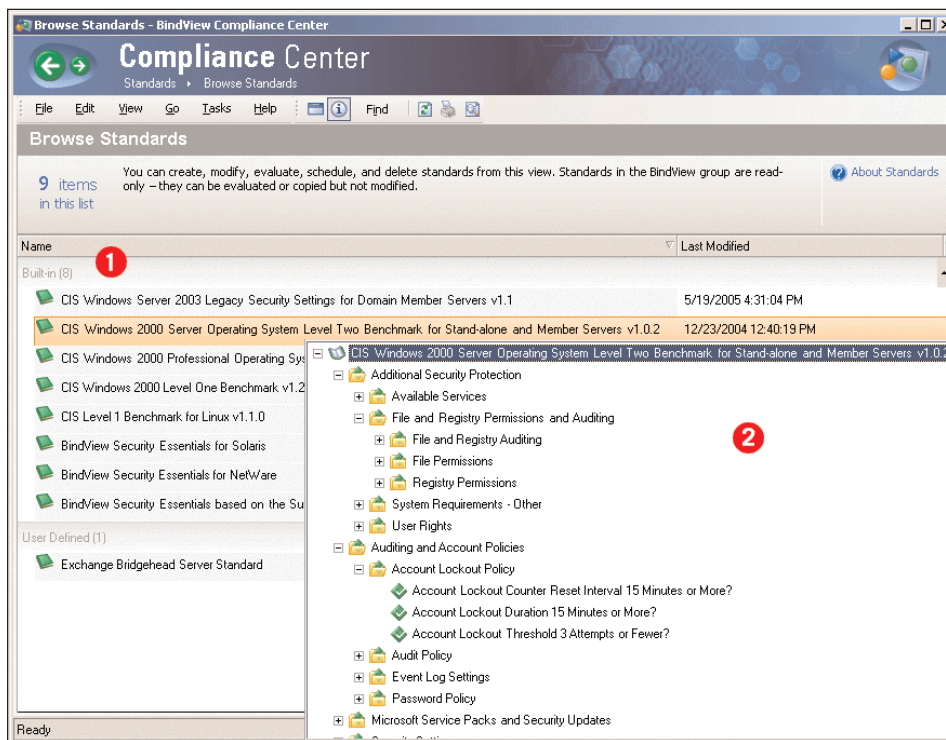
**Directory & Access Management:** Satisfying regulatory mandates requires managing and implementing proper identity and access controls throughout your organization. Symantec's award-winning Directory & Access Management solutions deliver the capabilities to audit access, provision users, manage user-based policies for security, privacy and confidentiality, as well as enable self-service administration.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### Compliance Made Visible with Symantec

One of the unique strengths of Symantec compliance solutions lies in the ability to help you automate, illuminate and demonstrate compliance through high-level and detailed reports.

Symantec Compliance Manager helps you to demonstrate compliance through a collection of automated checks that map directly to accepted industry security standards. This enables you to document compliance and demonstrate due care to interested parties such as internal or external auditors, with dashboard views that display percentage compliance across the enterprise. Symantec's built-in best practice knowledge provides an excellent starting point for securing systems and serves as an efficient means to compare your company's internal standards with accepted industry standards.

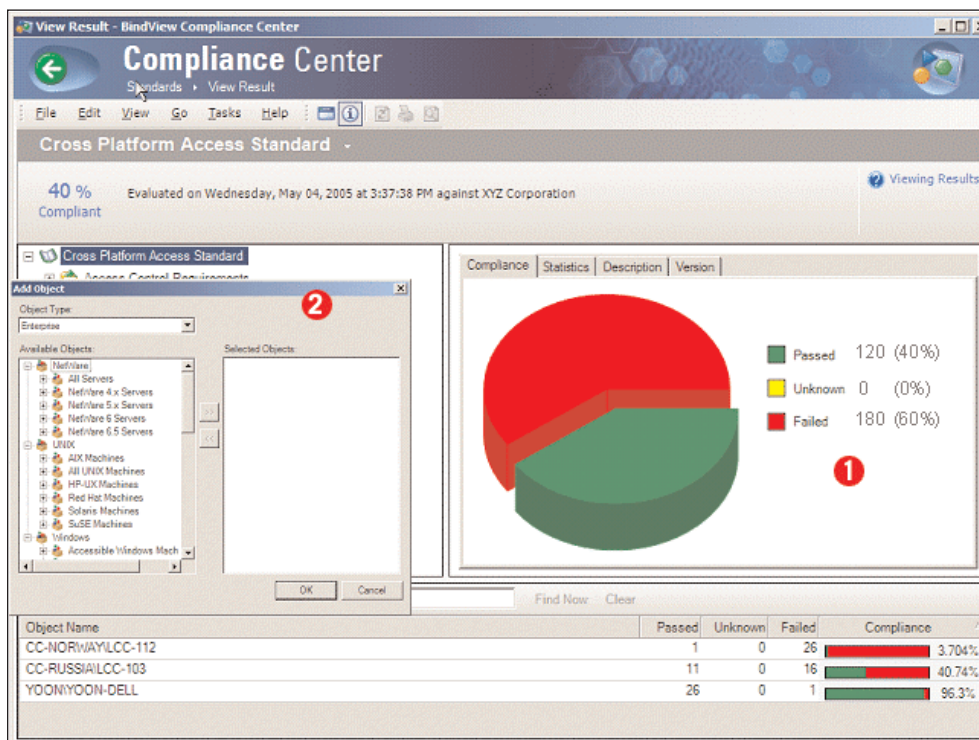


**Figure 6 - Compliance Evaluation to an Industry Standard**

Symantec Compliance Manager displays a detailed view of the requirements within the CIS Level 2 for Windows® 2000 Server benchmark. When running a report using these technical standards, you receive an overall compliance score. Standards can be modified to fit your unique environment, allowing you to select the requirements you want to measure, or to create additional requirements that augment these built-in standards.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

Symantec Compliance Center allows you to measure compliance against accepted industry standards such as CIS Level-1 and Level-2 benchmarks, as well as your internal policies. Compliance Center helps you assess, monitor, and report on your security status across multiple platforms, making high-level compliance reviews of the entire enterprise easier and more efficient.



**Figure 7 - Compliance Evaluation for the Entire Enterprise**

A Security, IT, or Audit Director can quickly review a single compliance score covering multiple platforms across the enterprise. Compliance Center reporting supports all major operating systems including Windows®, UNIX®, Linux® and Novell®.

Keep in mind that Compliance Center can also provide a detailed evaluation of any single system, including a detailed checklist of non-compliant items and a fix report with instructions for how to correct these items. In addition, Compliance Center offers a convenient method for managing exceptions.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **Compliance Made Practical with Symantec**

A financial services company located in the Western U.S. uses Symantec software solutions to audit compliance with internal standards for more than 250 Windows® servers, and several NetWare®/NDS® servers that support multiple business units. Corporate policy requires each server to be audited twice a week for compliance with internal build standards—an impossible task with manual methods that would demand a minimum of 42 hours for just one audit check of all servers. After deploying bv-Control with Compliance Center from Symantec, however, security managers are now able to conduct the audit checks daily, spending 20 minutes or less when status has changed, and requiring less than a minute if server status has not changed.

### **Why Symantec**

#### **Demonstrate Compliance**

Once a compliance control structure is established and operational procedures and policies are documented, the compliance burden shifts to continuous IT infrastructure assessment, validation and monitoring. Regulators and auditors want to be assured that when gaps in a control structure become evident, the organization promptly identifies remediation tasks and completes them. Auditors also provide an independent analysis of gaps in the management of compliance architecture and associated programs. Organizations must therefore be able to automate processes that assure the ability to sustain compliance through continuous monitoring, reporting and remediation.

#### **Reduce Complexity**

Symantec compliance solutions for IT security controls are above all practical to deploy and maintain, helping to minimize complexity across your heterogeneous IT environment. By mapping regulatory security requirements to specific IT policies and controls, Symantec simplifies one of the most time-consuming and complex tasks of compliance. In addition, our agent-less software also helps to reduce the complexity and burden on your IT infrastructure, while our automated tools simplify complex and manually intensive procedures so that you get the information you need rapidly and in easy-to-understand formats that can be communicated to all levels of your organization.

## Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs

### **Lower Costs**

Recognizing that IT-related compliance tasks require substantial time and effort—and that many of these tasks must be performed weekly or even daily—Symantec delivers solutions that enable you to substantially reduce the cost of compliance. By automating procedures to help you continuously monitor and report on your compliance posture, Symantec enables you to sustain and improve your compliance efforts and IT security over time at the lowest possible cost.

### **Customer Success**

With more than 5,000 customers across the globe, Symantec is dedicated to sharing the insights of your professional colleagues with you through online training and events such as our annual user conference. Through the exchange of practical techniques for implementing IT controls for compliance, Symantec helps you to understand and take advantage of successful methods using our proven solutions.

### **Getting Started with Symantec**

Regardless of where your organization may find itself on the compliance continuum, or at what stage you may be in the compliance challenge process, Symantec can help. For those facing immediate or imminent compliance audits, Symantec software and professional services provide solutions that can be implemented in a matter of days or weeks versus months. For those who may have completed an initial compliance audit process, Symantec can help to substantially reduce the costs of maintaining and demonstrating compliance on a continuous basis.

---

### **References**

1. Computer Security Institute/FBI Annual Computer Crime and Security Survey. [www.gocsi.com/forms/fbi/csi\\_fbi\\_survey.jhtml](http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml).
2. "Add it Up: Compliance Doesn't Come Cheap," Steve Marlin, *InformationWeek*, March 21, 2005.
3. "Attack of the Auditors," Oliver Rist, *InfoWorld*, March 21, 2005.
4. "Sarbanes-Oxley Security and Risk Controls: When is Enough Enough?" Webcast, Paul Proctor, December 14, 2004.
5. The Center for Internet Security. [www.cisecurity.org](http://www.cisecurity.org).

## About Symantec

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, California, Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517-8000  
1 (800) 721-3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
01/06

10527720