



Best Practices for Meeting the Challenge of IT Compliance

Guidelines to help you comply with multiple regulations, lower the cost of compliance, and reduce the risk of noncompliance

Ravi Sundararajan
Senior Director, Product Management
Symantec Corporation

Jim Hurley
Managing Director
Security Compliance Council

Best Practices for Meeting the Challenge of IT Compliance

Guidelines to help you comply with multiple regulations, lower the cost of compliance, and reduce the risk of noncompliance

Contents

Introduction	4
Defining IT compliance	4
Information security	5
Content management	5
Policies and procedures	6
The IT compliance challenge	6
Growing complexity of managing compliance with multiple regulations	6
Increasing costs of compliance	8
Risks posed by noncompliance	9
Meeting the IT compliance challenge	9
Select a framework to facilitate compliance with multiple regulations	10
Use automation to reduce compliance costs	10
Apply best practices to reduce risk	10
Measuring compliance performance	11
Lessons to be learned from leaders and laggards	11
Best-practice recommendations to reduce risk	12
Symantec solution offering	14
Define, document, and disseminate	16
Implement and sustain controls	17
Govern compliance and improve control environment	19
Conclusion	20
Appendix	21

Introduction

Compliance. Corporate governance. Enterprise risk management. Regardless of company size, industry, or geographic location, these phrases have become an integral part of most business objectives and initiatives, from the boardroom to the data center. Although the term *compliance* has many interpretations, the intent of multiple regulations, industry standards, and best practices frameworks is to achieve a common result: to ensure the security, the availability, and ultimately the integrity of business information.

This white paper is intended to help CIOs align their information technology (IT) infrastructure and security to meet the business requirements set forth by the many functions involved in the compliance process. The goal is to create a sound control environment that supports the business and addresses IT risks efficiently.

To help organizations improve their IT compliance processes, research has been conducted recently by the Security Compliance Council (www.SecurityCompliance.com) to help identify and articulate best practices. This paper reviews the latest research and highlights compliance practices in three categories: industry leaders, those representing the industry norm, and industry laggards.

This paper then describes how best-practice guidelines are incorporated into the Symantec IT Compliance process model and its solutions. It explains how organizations can use these solutions to implement more effective and efficient IT controls that will satisfy auditors and meet regulatory compliance and business mandates.

Defining IT compliance

IT compliance addresses external regulations, industry standards, frameworks, and internal corporate policies that require IT controls around the creation, retention, disclosure, protection, and integrity of information. Addressing compliance with external laws, regulations, and standards, as well as with internal policies, is a cross-functional effort involving multiple internal and external stakeholders.

Generally, IT compliance can be categorized into three distinct areas:

- Information security
- Content management
- Policies and procedures

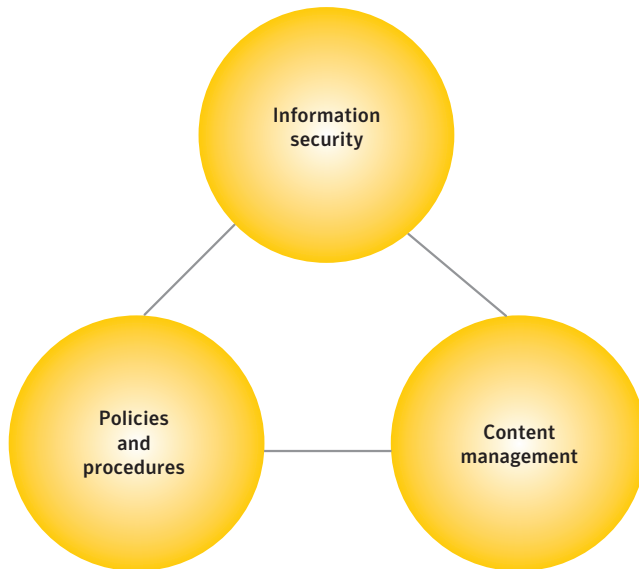


Figure 1. The three cornerstones of IT compliance are information security, content management, and policies and procedures.

Source: Financial Insights, 2006

Information security

Information security is the backbone of any compliance infrastructure. Without effective security controls, organizations expose proprietary information and their customers' personal information to the dangers of theft or unauthorized access, which can lead to disastrous consequences. Theft of customer financial information, for example, can result in fraud, money laundering, or even financing of illicit activities.

Information security is a dynamic process. Attacks against systems evolve as hackers and criminals continually identify new methods and techniques to break through the protection of security controls. As a result, the most important part of an information security program is to implement processes that continually assess security risks, and to respond to these risks as quickly as possible with stronger controls.

Content management

Content management is a critical component of any organization's record retention strategy. Content management involves the indexing, storage, and retrieval of business records. While storage and backup solutions are critical components of compliance solutions, organizations also need to consider higher-level content management solutions, including those for archiving and document or records management.

Best Practices for Meeting the Challenge of IT Compliance

Content management solutions must enable firms to automate the enforcement of retention policies by setting expiration dates on documents, prohibiting deletion before the retention period expires, and purging records upon expiration. Message archive solutions should also monitor communications through mediums such as email or instant messaging to help detect noncompliance or any attempt to tamper with or alter original messages.

Policies and procedures

Since lawmakers and regulators purposely do not dictate how compliance should be accomplished, regulations typically provide the destination, rather than the roadmap to achieving compliance. Therefore, it is up to each organization to determine the policies and procedures that best fit its individual requirements.

As part of the process, organizations must clearly define and articulate the policies and procedures that are required to support compliance initiatives. Organizations must ensure that employees are properly trained on policies and informed when changes occur. Participation—through input and enforcement—from the top to the bottom of the organization is critical to ensuring success, and this includes the involvement of IT as well as business units.

The IT compliance challenge

Recent research conducted by SecurityCompliance.com indicates several major challenges that organizations face in meeting the requirements for IT compliance:

1. Growing complexity of managing compliance with multiple regulations
2. Increasing costs of compliance
3. Risks posed by noncompliance

Growing complexity of managing compliance with multiple regulations

The pressure to demonstrate compliance with regulatory mandates has continued to increase over the past several years, with some organizations now subject to five or more regulatory mandates. Nearly half of the organizations surveyed by SecurityCompliance.com, however, are currently subject to three “most pressing” regulatory compliance mandates requiring that they demonstrate IT security through internal or external audits.¹ (See Figure 2.)

¹ “The Struggle to Manage Security Compliance for Multiple Regulations,” www.securitycompliance.com, January 2006.

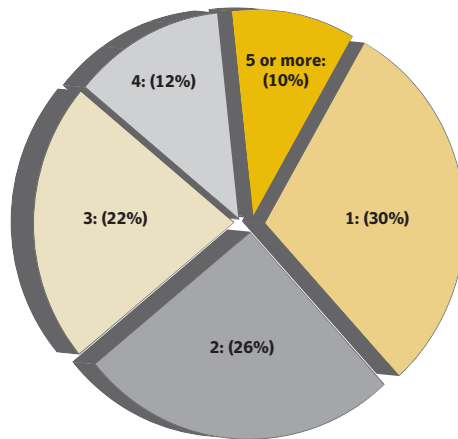


Figure 2. Percentage of companies subject to one or more mandates. Nearly half of all companies surveyed are now subject to three mandates or more.

Source: www.SecurityCompliance.com

With so many organizations struggling to meet audits that must satisfy multiple regulatory mandates, vast amounts of IT resources are being spent specifically to demonstrate IT security compliance with regulatory requirements. On average, more than one third (34 percent) of IT resources are being spent on meeting multiple regulatory compliance demands, according to SecurityCompliance.com. The analyst firm AMR Research, for example, estimates that compliance spending will exceed \$80 billion over the next five years and \$15.5 billion this year. For 2005, AMR says companies spent \$5.8 billion on meeting Sarbanes-Oxley requirements alone.²

Acting as a “hidden tax on profits,” the IT resources dedicated to satisfying audits are directly impacting the corporate bottom line and an organization’s ability to do business. The impact on the IT department, for example, can include delays on projects that would otherwise materially benefit the organization, such as new business procedures, new applications, new partner networks, and new customer sales and service programs. The labor-intensive nature of demonstrating regulatory compliance in IT also acts to constrain top-line growth while delaying efficiencies that could be achieved through the automation of variable costs.

² “Add it Up: Compliance Doesn’t Come Cheap,” Steve Marlin, *InformationWeek*, March 21, 2005.

Increasing costs of compliance

There are several factors that contribute to the increasing costs of compliance in terms of IT resources and budget. Manual, ad hoc processes, for example, are one of the most common contributors to the increasing cost of compliance. In many organizations, manual processes exist throughout the entire IT compliance process, creating labor-intensive activities that are expensive, error-prone, and not easily repeatable. Table 1 illustrates several manual ad hoc processes that add to the cost of compliance.

Scenario	Current process
Policy documentation, dissemination, and management	Multiple internal stakeholders are involved in the policy creation process. Unfortunately, the manual process of documentation, getting the appropriate approvals, and enforcing adherence to policies in a consistent way is not effective when using various Microsoft® Excel® spreadsheets and Word documents scattered throughout the organization.
Translation from business requirement to technical controls	Once policies are defined, the effort of translating them into actual technical controls and triggers is complicated and cumbersome. The time spent translating policy into auditable processes, sorting through and integrating the plethora of tools and data, and managing remediation and communication by hand represents a significant cost to the enterprise.
Reporting	If the effectiveness of the control environment can't be tested and reported on, it's not a valid control. However, demonstrating compliance in today's complex IT environment with too many tools and too much data is not an efficient process. Often, too much time is spent bringing these disparate elements together to analyze the results.

Table 1. Scenarios that demonstrate manual ad hoc processes.

In addition to manual processes, inconsistent processes among business units and geographies also create fragmented compliance initiatives that result in inefficiencies. Compliance initiatives managed by different groups in separate departments can mean duplicate efforts to test, measure, and report on the same IT control function across the organization. These duplicate efforts require more internal IT time to prepare for an audit, and require more time from external auditors to properly evaluate the control environment, resulting in increased audit fees. In addition, managing each compliance initiative in an isolated or “silo” approach creates pockets of discrete information that are rarely leveraged at the corporate level.

Risks posed by noncompliance

In the past few years, regulators have become more aggressive in penalizing firms for failing to disclose, retain, or secure information of various types under new guidance, regulations, and laws. This increase in enforcement may stem from criticism in the media and by legislators that regulators have not effectively prevented or responded to failures in corporate governance as reflected in high-profile bankruptcies. In many cases, however, failures in governance are not necessarily driven by an organization's desire to deceive, but rather are due to its lack of policies and procedures or its failure to detect the fraudulent activities among its employees.

Besides complying with evolving regulatory, legal, or industry standards, organizations also face the challenge of managing ever-growing amounts of information. The most significant challenge is not necessarily in storing this information—firms can always add more storage capacity since the cost of storage devices has been decreasing at more than 50 percent per year since 1997.

Rather, the challenge comes from properly managing information so that important documents and data are retained in accordance with an appropriate time frame and are readily accessible to those who need to review them. Simply storing all information in storage servers is no longer an acceptable option. When information critical to the business or to legal discovery is not securely stored and readily available, the risk of noncompliance increases.

Because most regulations are necessarily vague, organizations are on their own when it comes to finding guidance on IT requirements and mapping those requirements to specific policies and control objectives. The problem only gets more complex when multiple mandates must be managed simultaneously.

Thus, many organizations today find themselves facing IT compliance challenges that must be resolved in order to:

- Establish and sustain compliance with multiple, changing regulations
- Reduce the high cost of being compliant
- Minimize the risks of noncompliance

Meeting the IT compliance challenge

In response to IT compliance challenges, firms are attempting to minimize fragmented initiatives, automate audit procedures and IT security controls to reduce labor and consultant costs, and increase the frequency of internal audits to sustain hard-won compliance profiles. The goal of these organizations is to comply with regulatory requirements more cost effectively, so that they can allocate IT resources to more productive pursuits.

Select a framework to facilitate compliance with multiple regulations

While the basics of demonstrating compliance are similar across multiple mandates, managing the details and discovering commonalities or overlaps in controls is a complex problem. Reusing control data across multiple reports and delivering evidence of compliance to regulatory bodies can require a substantial investment in upfront time and effort. However, applying security policies based on ISO 17799 or a similar recognized and accepted security framework enables the organization to utilize one set of policy rules to help manage its entire compliance effort.

To develop a sustainable compliance posture, organizations are recognizing the value of implementing an overall control framework such as COSO, COBIT, or ISO 17799. Adoption of such a framework simplifies communication, validates the controls with auditors and regulators, and reduces the effort required and therefore the cost to the enterprise.

Use automation to reduce compliance costs

While there are many ways to reduce the costs of compliance, the use of technology to automate and consolidate many manual activities can reduce significantly the amount of time and money spent on compliance. Through a sound IT-control architecture; strong policies; and the use of technology solutions capable of managing, maintaining, and reporting on the status of compliance, organizations can reduce the human and monetary resources required for compliance.

Research by SecurityCompliance.com shows that two-thirds of firms are already attempting to automate audit procedures and IT security controls to help reduce labor costs and allow IT to focus on more productive pursuits. Unfortunately, the same survey found that more than one quarter of organizations continue to rely on costly manual methods.

Apply best practices to reduce risk

As large numbers of organizations have committed extensive resources to achieving compliance with regulations such as the Sarbanes-Oxley Act, the Health Information Portability and Accountability Act of 1996, and others in the past several years, our real-world knowledge and experience has grown. To tap into this vast storehouse of experience, the Security Compliance Council at www.securitycompliance.com has conducted research to help identify and describe best practices in IT compliance. This research is, in turn, helping to establish performance benchmarks that all organizations can use to help improve their own efforts to achieve compliance with multiple regulations.

Measuring compliance performance

How does an organization effectively measure its compliance performance? For the vast majority, performance in achieving compliance is measured by means of a negative: the number of “significant and material” deficiencies identified through the audit process. The fewer deficiencies discovered, the better the organization’s performance in achieving compliance.

Although the pressure to demonstrate compliance is shared by all organizations, performance results in the real world appear to vary significantly. Research in early 2006 by the Security Compliance Council indicates that only 11 percent of organizations (about one in ten) are achieving superior performance results and could be considered “leaders” when measured by audits that tally their overall “significant and material” deficiencies. In contrast, about twice as many survey respondents (23 percent) were considered “laggards.” The majority of organizations (66 percent) performed at industry norms.³

Industry benchmarks from this research were based on regulatory audit results that show:

- One in ten firms with 2 significant and material deficiencies (leaders)
- Seven out of ten firms with 6 significant and material deficiencies (norm)
- Two out of ten firms with 33 significant and material deficiencies (laggards)

Lessons to be learned from leaders and laggards

The research revealed that performing as a leader costs more time and money, and includes the potential of lost opportunity when managers focus IT resources on demonstrating compliance rather than on activities that would impact revenue and growth.

Performing as a laggard, however, also has its costs. According to the research, these costs manifest themselves in terms of decreased public trust in the organization and its brand among customers, concern about the accuracy of quarterly financial statements, and the potential impact of noncompliance sanctions or penalties on the organization and its executive management.

³ “Improving Performance Results to Achieve Regulatory Compliance: 2006 Security Compliance Performance Benchmark Report,” www.securitycompliance.com, May 2006.

Best Practices for Meeting the Challenge of IT Compliance

Success Factors	Laggards (23%)	Norm (67%)	Leaders (10%)
Frequency of internal audits	8 Months	7 Months	1 Month
IT time spent on compliance	16%	25%	30%
IT budget spent on security	4.5%	7.4%	12.7%
Number of overall deficiencies	75	30	20
Number of significant deficiencies	33	6	2

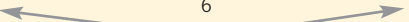


Table 2. Comparison of success factors in achieving compliance.

As the research shows in Table 2, leaders in achieving IT compliance (i.e., those with the fewest audit deficiencies) are 15 times more effective than laggards, even though they spend only about three times more than laggards to achieve that effectiveness. We can see from the table that more frequent auditing, monitoring, and reporting translate into better IT security practices and therefore better protection for an organization.

Beyond simply quantifying regulatory pressures to which organizations are responding, benchmark research has helped quantify the relationship between performance results and the actions that organizations are taking to achieve their results. These research findings clearly demonstrate a link between performance results and a few critical success factors that illustrate what is working across many organizations.

Best-practice recommendations to reduce risk

Based on the success factors listed in Table 2, compliance benchmark research offers several suggestions for actions that have been shown to improve results for IT security and regulatory compliance.

Conduct internal regulatory and IT security audits at least monthly

Industry leaders are conducting internal audit and IT security monitoring, on average, at least once a month. That's eight times more frequently than the industry laggards and seven times more frequently than firms operating at the industry norm. As a result, leaders are experiencing "significant and material" deficiency levels that are sixteen times better (lower) than those of the laggards. Frequency of audit by itself, however, is not the only factor responsible for achieving improved performance in regulatory compliance.

Best Practices for Meeting the Challenge of IT Compliance

Spend at least 25 percent of IT staff time on regulatory compliance

Industry leaders are allocating 30 percent of IT staff time to regulatory compliance. In comparison, companies performing at the industry norm are allocating 25 percent of staff time to regulatory compliance, while industry laggards are allocating only 16 percent. Based on 250 work days a year, this translates to a little over six days per month among the leaders, five days per month among the norm, and about three days per month among the laggards.

Allocate more than 10 percent of the IT budget to IT security

Industry leaders are spending 170 percent more on IT security, are experiencing substantially fewer (300 percent) “significant and material” deficiencies than are firms performing at the industry norm, and 1,000 percent fewer deficiencies than laggards. Despite the link between spending and IT staff time devoted to compliance, how the money is spent on IT security and where the time is focused differentiates performance results among firms operating as leaders, at the industry norm, and as laggards.

Establish clear objectives and measure results at regular intervals

Leading organizations are measuring results monthly and managing deficiencies to achieve and sustain compliance. Roles and responsibilities for compliance are clearly defined and objectives are measurable. In contrast, procedures for demonstrating regulatory compliance among laggards and normative firms are rarely defined and are mostly manual. Among the laggards, data and knowledge about compliance is rarely managed.

Automate compliance and IT security controls and procedures with IT technology tools

Nearly all IT security technology controls and procedures are now automated among the organizations performing as leaders in compliance. Although most firms are improving IT security policies, standards, and documentation, the leaders are singularly focused on documenting procedures, making changes to both business and technical procedures, and automating these processes as much as possible.

Symantec solution offering

According to research from the Security Compliance Council, the major priorities for improving performance in achieving regulatory compliance include identifying repeatable and more efficient methods to demonstrate compliance; using technology to automate IT security, audit, and compliance procedures; and improving risk management practices for information assets.

The following section describes how Symantec is uniquely positioned to help you simplify and sustain compliance across your organization with a consolidated view of IT compliance, proactive and reliable IT controls, and actionable intelligence.

The Symantec IT compliance solution includes products that address the major challenges facing any organization seeking to improve its performance by:

- Minimizing the complexity of complying with multiple regulations by providing a single, consistent view of IT compliance through common policies and IT controls across various mandates
- Reducing the time and cost of demonstrating compliance by centralizing intelligence across IT efforts to improve decision-making and prove ongoing compliance with confidence
- Mitigating the risk of noncompliance by implementing and managing IT controls in the most efficient, least complex manner to increase the effectiveness and reliability of IT controls across the infrastructure

The top portion of Figure 3 illustrates a sustainable IT compliance process across multiple initiatives. The bottom portion shows Symantec offerings that correspond with the IT compliance process. As the figure shows, Symantec offers solutions at each phase of the process to help you define, control, and govern policies with proven best practices. In addition, Symantec solutions cover comprehensively the major functions of IT compliance in terms of developing policies and procedures, ensuring information security, and implementing content management.

Best Practices for Meeting the Challenge of IT Compliance

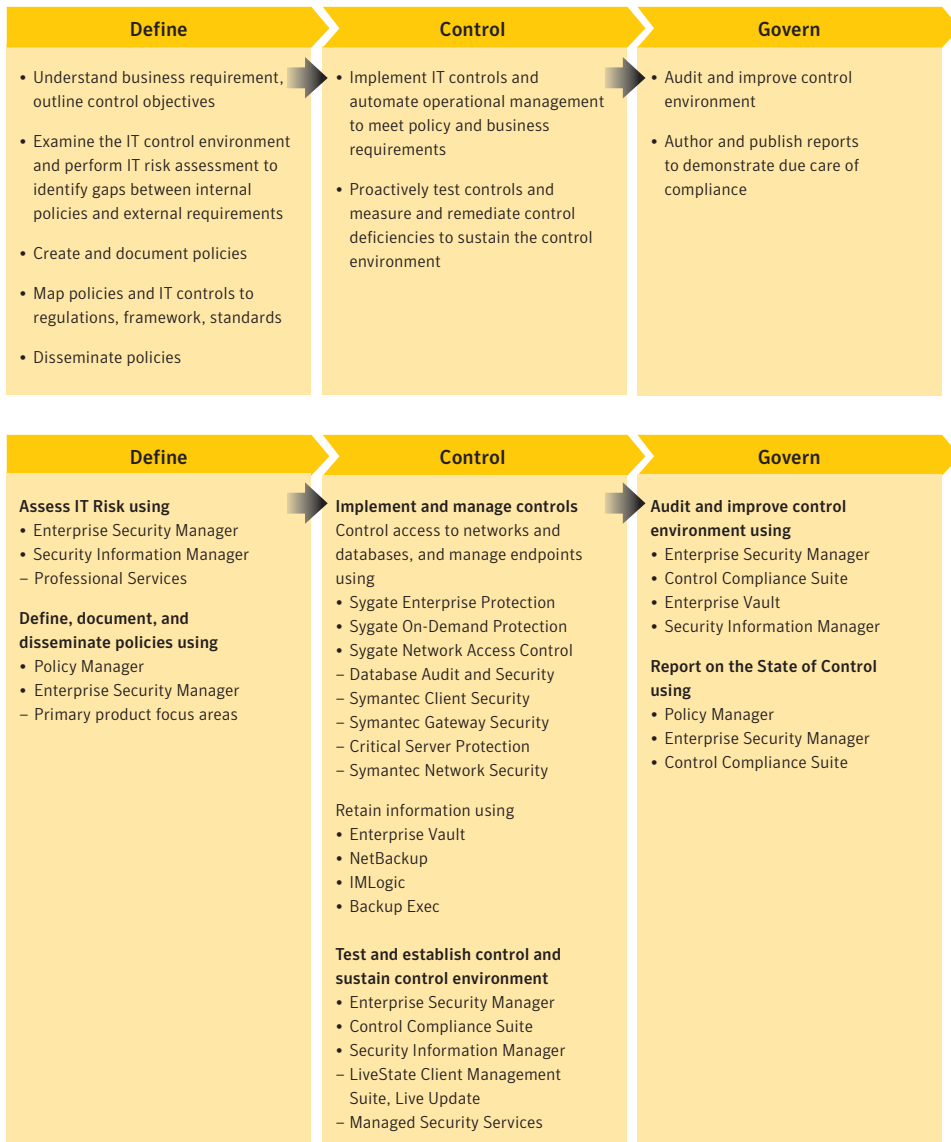


Figure 3. Sustainable IT compliance process and corresponding Symantec offerings.

Define, document, and disseminate

The process of defining controls for compliance is complex, since regulations are not specific when it comes to the exact controls necessary to satisfy auditors and regulators. Regulations are constantly changing and evolving and must be translated and mapped to specific IT controls, documented, and then enforced consistently throughout the organization's technical infrastructure and among its people.

The definition phase encompasses the following processes:

- Understanding the business requirements
- Outlining the control objectives
- Assessing business risk
- Examining the IT control environment
- Performing IT risk assessment to identify gaps in the control structure
- Creating and documenting policies
- Mapping policies and IT controls to regulations, frameworks, and standards
- Disseminating policies

Table 3 describes Symantec products that provide value to processes in the definition phase of IT compliance.

Symantec product	Value for the definition phase
Symantec BindView™ Policy Manager	Automates the process of creating and disseminating policy throughout the organization. Assesses compliance with multiple regulations using a single set of universal and actionable IT controls.
Veritas Enterprise Vault™	Defines and documents retention policies based upon the type of business record.
Enterprise Security Manager™ and Control Compliance Suite	Creates and documents IT security policy checks aligned to controls and monitors changes to control structure.
Symantec Enterprise Security Manager Solution Assessment Service	Assesses the organization's people, processes, and technology to improve management of technical compliance.
Symantec Security Information Manager	Discovers assets and assigns CIA values to each asset being monitored for a risk-based, real-time assessment of threats.

Table 3. Primary Symantec products for the definition phase of IT compliance.

Implement and sustain controls

The key to IT compliance is found in the documentation, monitoring, and management of a control structure for your specific IT 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, who often want to see documentary evidence and may even want to conduct onsite tests of the controls.

Regulators and auditors also want to be assured that when gaps in a control structure become evident, the organization promptly identifies remediation tasks and completes them. Your compliance control structure establishes accountability, responsibility, and risk management principles that are carried out at the IT control level to assure policy enforcement.

The control phase includes the following processes:

- Implementing IT controls
- Automating the operational management of IT controls to meet policy and business requirements
- Proactively measuring and remediating deficiencies to sustain the control environment

Technically, any product Symantec offers can be considered an IT control. The implementation of each control is based upon the IT environment unique to the company. Table 4 shows the Symantec products that provide value to processes in the control phase.

Best Practices for Meeting the Challenge of IT Compliance

Symantec product	Value for the control phase
Symantec BindView Policy Manager	Assesses compliance with written policy through integration with management software.
Enterprise Security Manager and Control Compliance Suite	Provides specific configuration settings mapped to IT policies that enable you to implement controls across a heterogeneous IT infrastructure and automate the comprehensive assessment of compliance to IT policies across platforms and applications with a single tool. Provides recommendations for remediation of risks or holes in an organization's security posture.
Symantec Sygate™ Enterprise Protection	Provides advanced endpoint protection and seamless integration with network access control in a single management architecture. Protects managed endpoints against unknown or emerging attacks with desktop firewall, host-based intrusion prevention, and adaptive protection technologies, while simultaneously securing networks against noncompliant endpoints and enforcing compliance on contact.
Symantec Sygate On Demand Protection	Helps prevent the compromise of enterprise assets such as company financials, customer information, and intellectual property caused by unprotected network access through Web-enabled applications, wireless LANs, and SSL VPNs by unmanaged devices, including home computers, kiosks, and guest laptops.
Symantec On-Demand Protection Solution Symantec Sygate Network Access Control	Blocks or quarantines noncompliant devices attempting to access the corporate network and resources.
Symantec Database Audit and Security	Monitors all database access and traffic based upon behavior and policies to detect critical information leaving the database inappropriately.
Veritas Enterprise Vault	Enables organizations to more effectively manage email and other forms of unstructured electronic content by providing a secure, searchable online archive for critical business records.
Veritas NetBackup™	Delivers high-performance data protection that scales to protect the largest UNIX®, Microsoft Windows®, Linux®, and NetWare® environments. Offers complete protection from desktop to data center to vault, giving companies a single management tool to consolidate all backup and recovery operations, while providing cutting-edge management, alerting, reporting, and troubleshooting technologies.
Symantec LiveState™ Client Management Suite	Offers a comprehensive solution to discover, provision, configure, patch, and recover client devices. Keeps them secure, available, and compliant with corporate standards, from acquisition to disposal.
Symantec Security Information Manager	Enables automatic identification and prioritization of security threats that impact business-critical applications and aligns incident response with IT helpdesk workflow processes to ensure compliance with corporate security policies.

Table 4. Primary Symantec products for the control phase of IT compliance.

Govern compliance and improve control environment

Once a compliance control structure is established and operational procedures and policies are implemented, the compliance burden shifts to continuous assessment, validation, and improvement of the IT infrastructure. Good governance requires a constant analysis of gaps in the management of the compliance architecture and associated programs. Organizations must therefore be able to automate processes that are able to sustain compliance through continuous monitoring, reporting, and improvement of the control environment.

The governing phase includes the following processes:

- Audit and examine the control environment
- Author and publish reports to demonstrate due care for compliance
- Provide recommendations for improvements to the control environment

Table 5 describes Symantec products that provide value to processes in the governing phase.

Symantec product	Value for the governing phase
Enterprise Security Manager and Control Compliance Suite	Tracks and trends compliance levels over time per policy, providing auditors with a single interface to evaluate IT compliance posture. Reports on policy coverage gaps as required by a regulation, framework, or control objective.
Symantec BindView Policy Manager	Reports on policy coverage gaps according to regulation or framework, leveraging out-of-the-box reports to help determine policy coverage, policy awareness, and policy efficacy and incorporating generally accepted best-practice standards. This enables you to leverage the same information used by your auditors when they validate compliance.
Symantec Security Information Manager	Automates the collection and retention of consolidated raw log data for forensics purposes.
Veritas Enterprise Vault	Enables compliance with industry and government regulations and laws requiring the retention and supervision of email. In addition, built-in, powerful search and discovery capabilities manage content via automated, policy-controlled archiving to online stores for active retention and seamless retrieval of information when requested by senior management, auditors, or legal as part of discovery.

Table 5. Primary Symantec products for the governing phase of IT compliance.

Conclusion: Will you be a leader or a laggard?

Establishing and sustaining IT compliance is a journey rather than a destination. By constantly learning about how organizations are planning and implementing IT compliance processes and controls, you can take advantage of the hard-earned insights of organizations like yours. As a major participant in the Security Compliance Council, Symantec is dedicated to providing you with the latest information on IT compliance best practices and benchmarks through ongoing research.

As you strive to improve your IT compliance performance, keep in mind that Symantec solutions address the major challenges facing your organization, helping you to:

- Minimize the complexity of navigating multiple regulations by providing a single, consistent view of IT compliance through common policies and IT controls
- Reduce the time and cost of demonstrating compliance by centralizing and automating intelligence across IT efforts, improving decision-making and proving ongoing compliance with confidence
- Mitigate the risk of noncompliance by implementing and managing IT controls in the most efficient, least complex manner to increase the effectiveness and reliability of IT controls across the infrastructure

Appendix—Glossary

- **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 operation of the organization. Policies typically include general statements of goals, objectives, beliefs, ethics, controls, and worker responsibilities.
- **Regulation**—A mandate 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 loss of accreditation. Regulations typically refer to frameworks and standards for practical application and demonstration of compliance.
- **Framework**—A methodology for performing an evaluation, typically created by an industry leader or a consortium of auditing entities. Frameworks are the prescribed method of evaluating 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.”

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at 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

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, BindView, Enterprise Security Manager, Sygate, Veritas, Enterprise Vault, NetBackup and LiveState 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. Printed in the USA. 06/06 10579577