



Creating scalable, repeatable, and sustainable infrastructure controls assessments

Technical Brief

Creating scalable, repeatable, and sustainable infrastructure controls assessments

Contents

Executive summary	4
The increasing demand for compliance	4
The challenges of sustaining compliance	6
Challenges: Managing security controls in the Microsoft environment	7
The components of a sustainable solution	9
The value of Symantec Control Compliance Suite	12
Segregation of duties	12
Configuration management	13
Resource management	14
Integration with Symantec Bindview Policy Manager	15
Conclusion	15

Executive summary

Over the past several years, the profile of information security has increased significantly throughout many organizations, specifically in regard to the way information security supports an organization's internal control environment. Discussions of these issues are now taking place among upper management and at the executive board level, thereby increasing the need for timely, accurate, and relevant information about the organization's current security posture and plans for improvement. Further, an increasing number of industry guidelines and federal regulations require organizations to demonstrate compliance with established controls. Organizations have recognized the requirement to provide periodic security information, and have been looking to develop processes and deploy technologies to collect, communicate, and sustain security compliance programs.

While there is no single product that can address all the disparate and often competing requirements, the Symantec™ Control Compliance Suite provides a flexible and robust component of a repeatable and sustainable solution.

The increasing demand for compliance

To demonstrate that an environment has sufficient internal controls, it has become critical for organizations to define, measure, and report on the compliance of infrastructure and software applications with established security controls. Instances of noncompliance must be identified, evaluated for risk, and addressed appropriately to ensure that the control environment is maintained. There are a number of regulations that have had a significant impact on information security. These regulations have required organizations to focus on:

1. Integrating the requirements into their organization's information security policy
2. Monitoring for incidents
3. Reporting and demonstrating compliance
4. Performing remediation on noncompliant systems

This paper will detail two specific regulations: Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA).

Sarbanes-Oxley section 302 does not end with the requirement to implement internal controls. Sections 302(a)(4)(C) and (D) require the chief financial officer and chief executive to certify that they have evaluated the effectiveness of the [organization's] internal controls as of a date within 90 days prior to the report [in which their certification appears] (C); and have

Creating scalable, repeatable, and sustainable infrastructure controls assessments

presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date (D).

Similarly, Section 404(a)(2) of SOX requires that each company assess annually “the effectiveness of the internal control structure and procedures ... for financial reporting” for the purpose of preparing its annual “internal controls report.”

The Gramm-Leach-Bliley Act and its specifications present a varying set of legal requirements. Passed by Congress due to growing concerns over identity theft and misuse of consumer financial information, the law requires financial institutions to adopt numerous measures concerning use, disclosure, and protection of the nonpublic, personally identifiable information of customers. Although much attention has been paid to the privacy provisions of GLBA (which require institutions to develop privacy policies and send privacy notices to customers), more concern lately has been generated among managers, officers, and directors of financial institutions over the information security provisions of GLBA, also known as the “financial institution safeguards.”

These provisions are described in Section 501(b), which states that the regulatory agencies and authorities that govern financial institutions shall establish administrative, technical, and physical safeguards to:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any client

In the context of an information security program, there are three capabilities that are considered fundamental security controls:

- Segregation of duties
- Configuration management
- Resource management

Segregation of duties requires the apportioning of tasks among different members of staff and provides oversight to reduce the scope for error and fraud. Configuration management is the process of identifying, recording, and reporting technical configurations with the goal of reducing complexity and cost. Resource management focuses on ensuring that users can only access those applications or resources to which they are entitled.

The challenges of sustaining compliance

Today, most organizations perform highly manual or partially automated processes to determine compliance. In complex, dynamic environments, these methods are resource intensive, error prone, and not extensible. As the size of the computing environment grows and new technologies are added, increasing amounts of time are necessary to collect and review configuration data to determine whether the systems meet the technical standards and therefore the corporate policies. Even when data collection is automated, the analysis requires specialized skills that are often already stretched thin. Further, as volume increases and time pressures remain constant, the mere fact that humans are performing the analysis leads to errors, including false positives, which cause extra work when following up on a non-issue, and false negatives, which provide an unsubstantiated level of comfort over the internal controls.

Finally, this method is neither scalable nor extensible, thereby requiring the organization to spend increased time and effort on incorporating new components into the environment and linking to other business processes.

When compliance processes are partially automated, the technologies selected often reduce the effort associated with certain tasks, but create more work in other areas. This occurs because these tools are not linked to the security policies of the organization or to each other. This partial automation generally occurs for the data collection task, which generates technical information that must then be compared to the security policies. The next step requires the preparation of appropriate reports and can be especially time-consuming. A major factor in this effort is the number of analyses and amount of data input to the reporting process.

For example, individual technology groups, functional groups, or business units use their own tools to collect data. These tools will produce output in differing formats, with different levels of detail, and may report differently for the same test. All of this input must be normalized, analyzed, and reported.

Finally, the reporting requirements themselves are becoming increasingly complex. Different regulations specify differing levels of detail and scope of coverage. Increased visibility in the organization requires an increased number of audience-specific reports. And, external and internal forces create a schedule of reporting deadlines that can include competing interests. For example, SOX requires reporting on “financially significant” systems, the FDA may be concerned with the systems participating in a clinical trial, while the government of California may be interested in systems holding personally identifiable, private customer information. These differing but sometimes overlapping scopes require increased time, resources, and interpretation to ensure that all the relevant items are reported.

Creating scalable, repeatable, and sustainable infrastructure controls assessments

Historically, technical compliance reporting was targeted at the technical staff that could perform remediation and improve consistency. Today, however, management and executives must receive reports that allow them to allocate resources and truly understand the posture of the organization. These reports are not simply different “cuts” of the same data; rather, they require interpretation and distillation of the data within the specific context of the business. On top of the increasingly complex reporting requirements are specifications for when and how often these reports will be generated and consumed.

The regulations themselves make specifications. According to SOX 302(a)(4)(C), the evaluation process must be conducted at least quarterly, and the effectiveness of the controls must be certified in writing by the chief executive and chief financial officer. Executives must receive effective reports that quantify the percentage of compliance and define variance within the organization. External and internal auditors will make their own specifications, while technical staff and management will have operational needs for frequent reports and periodic needs for continuous improvement.

Challenges: Managing security controls in the Microsoft® environment

Because of their high-profile vulnerabilities, widespread use across the desktop and infrastructure, and increasing use for critical business and operational systems, Microsoft Windows® environments represent a significant portion of the policy compliance and policy management challenge. The two major factors in this challenge are the high cost of maintaining multiple configurations and the risk associated with rogue and unmanaged systems.

Further, there are significant gaps between native and application software functionality available from Microsoft and the requirements of a robust security control management process. To properly control a computing environment, technical standards must be customized to address the type, function, and location of specific systems. For example, a file server needs different security controls than a domain controller, and both will be secured differently than an externally facing Web server.

Additionally, a business-critical system such as an Exchange mail server may have more stringent controls (which require more monitoring and maintenance) than a less important application server. In organizations that have implemented technologies for highly specialized purposes, specialized or customized controls must be implemented and maintained to sustain the security of the broader environment.

Creating scalable, repeatable, and sustainable infrastructure controls assessments

The other side of effective control is reducing the number of rogue and unmanaged systems. Any system that is outside the scope of scanning tools, configured by an individual or business unit without adhering to the corporate standard, or significantly altered after secure deployment creates an enormous risk to the overall control and security of the network. For example, if all servers except one were configured securely and were well controlled, but that one server became infected with a worm, it could create so much network traffic and bandwidth usage that other, critical systems would be unusable.

To this end, it is essential to ensure that, to the extent possible, all systems are monitored for compliance with policy and standards. And, for those systems that cannot be managed, other protections, such as physical and logical isolation and manual compliance activities, must be implemented.

In Windows environments, it is possible to gain access to domain resources and application services such as mail, file, and print without being subject to the controls of the Active Directory® (AD) service. Therefore, it is critical to have a process in place to identify unmanaged systems and determine whether they should be removed from the network, managed, or otherwise controlled.

As mentioned above, addressing these challenges within Windows environments has become an especially complex task and a high-priority initiative across organizations as concern focuses on new operating system vulnerabilities, automated connections to wireless LANs, integrated instant messaging, and remote desktop administration capabilities that can undermine existing controls. The impact on enterprise security can be profound if steps are not taken to implement a security infrastructure and secure environment. It is a fact that most intrusions arise from exploitation of known vulnerabilities and security weaknesses within software systems, most of which could have been avoided if security patches had been applied as they became available.

Microsoft provides a toolset with its operating systems and applications to perform a variety of operations and maintenance functions; however, these tools were not designed to address compliance needs as outlined above. While AD provides group policies to publish and enforce technical standards, it does not provide settings for all securable objects and does not inherently distinguish between server types. Additionally, if a machine is removed from the AD, then it will not receive group policies and administrators may not be alerted of this event. Active Directory, while feature rich in its infrastructure and operations capabilities, was not designed with compliance mechanisms and does not provide a robust set of reporting capabilities.

Creating scalable, repeatable, and sustainable infrastructure controls assessments

The Microsoft Security Configuration Editor, another native tool, can be used for some testing, but it must be run manually or scripted and can only scan one target at a time. Further, its scope is limited to system settings, which means it can miss Exchange, SQL, and other server application configurations, as well as desktop settings for applications such as Microsoft Outlook® and Office. To address some of these items, as well as to determine patch levels, Microsoft developed another tool, Microsoft Baseline Security Analyzer, in addition to its Systems Management Server and Windows Update Services. These tools are designed to scan networks and provide some reporting of configuration and patch levels and then provide mechanisms to update noncompliant systems. With all of these tools, it becomes increasingly complex to use just the available compliance features, normalize and integrate that information across the environment, and then produce meaningful reports.

Finally, to effectively prioritize and address compliance issues, decisions should be made about the risk and exposure level of systems. Native tools have no facility to provide this type of classification and prioritization.

Of course, these challenges become even greater when expanding beyond the Microsoft environment to include the UNIX®, Linux®, and Novell® operating systems—especially if an enterprise is managing all of them centrally.

The components of a sustainable solution

The fundamental building blocks of any effective business solution are people, processes, and technology. These are the supporting capabilities that provide the input for achieving business objectives. Since the relationship among these three elements determines the extent to which an enterprise can harness the value of security, their linkage is essential.

The people component consists of defining roles, responsibilities, and accountability, from the executives to the operations staff. It is important to understand the chain or matrix of command as well as funding, reporting, and operational responsibilities. The people concept also includes the training, education, and awareness of employees and contractors or vendors who fund, design, deploy, operate, administer, or maintain the enterprise's solution.

Creating scalable, repeatable, and sustainable infrastructure controls assessments

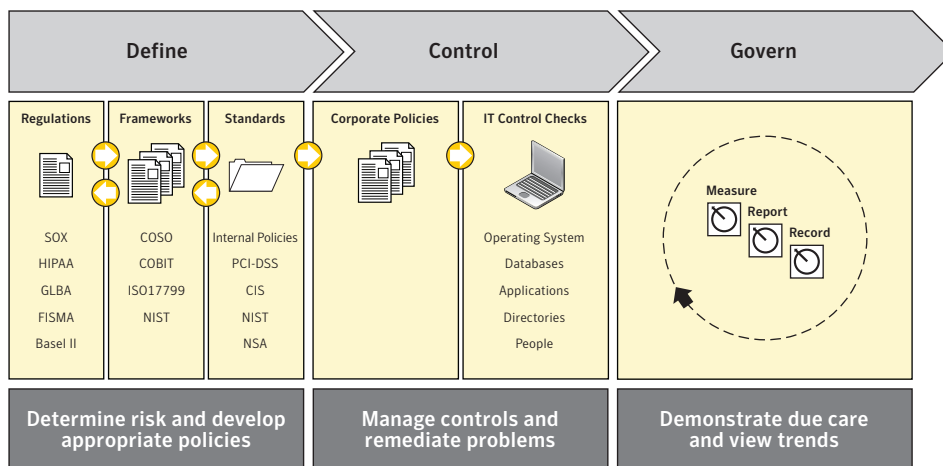


Figure 1. Symantec's comprehensive policy compliance approach helps ensure a sustainable process while reducing cost, through automation.

Once these roles are defined, a set of robust, measurable, repeatable processes must be developed to operate and maintain a secure, compliant environment. Clearly defined processes are critical because they enable scalability, skills leveraging, clear accountability, enterprisewide consistency in execution, measurability, and a basis for continuous improvement. These processes must therefore contain feedback mechanisms, handle failures and unexpected outcomes, and produce reports that comply with business and regulatory requirements.

Technologies can be used to automate some or all of the tasks required by the processes. It is important to note that technologies by themselves cannot solve business problems; they must be used to support defined processes and automation where appropriate. In the case of policy compliance, the data collection, normalization, and comparison to standards and policies can all be automated significantly. Report formats and schedules can also be automated. A tool specifically designed for this purpose, such as the Symantec Control Compliance Suite, can perform more effectively than native and disparate tool sets.

These capabilities support three major areas of control:

- Segregation of duties
- Configuration management
- Resource management

Creating scalable, repeatable, and sustainable infrastructure controls assessments

Business rules requiring segregation of duties can be implemented and maintained, ensuring that no single entity has control over the confidentiality, integrity, and/or availability of a resource. Specific tests can be performed to verify compliance with best-practice controls by testing for and comparing user authorities for proper segregations. These business rules provide a means of measuring and reporting on established security metrics through a consistent and structured methodology.

Symantec's second fundamental security capability is configuration management. This process enables a security organization to establish, track, and report on standardized system builds, finite system settings, enabled services, and file and directory permissions. Managing controls around system configurations helps an organization limit the risk of system interruptions or unexpected performance due to the presence of nonessential settings.

The third element of security control is resource management—the process of ensuring that users are given access only to those applications or resources that they are entitled to see or use. Effective implementation of this process enables the organization to provide appropriate levels of access to multiple and disparate information sources and applications and can reduce the overall operating costs associated with user access control.

In addition to improving the control environment, the development of these areas allows an organization to increase the value of its existing security products by acting as a point of consolidation for security business rules and determining compliance with those rules. Fundamental security capabilities can also improve the value of other security programs such as patch management, event management, and asset management by identifying nonpatched systems, feeding compliance issues to event management for resolution, and by establishing the security business rules for each IT asset.

A good compliance program leads to the improvement of other security capabilities through direct and indirect means. For example, when systems are compliant with best-practice technical standards, the risk associated with worms and other attacks based on known vulnerabilities is reduced. Strong security control management provides reporting capabilities that result in improved knowledge about the environment, including configuration data and risk levels. This increased data can feed an event- or change-management system that can dynamically prioritize events and incidents based on the importance of the system and its current control level. Finally, this threat, vulnerability, and compliance data can feed an asset management system that allows an organization to truly understand its technologies and therefore accurately determine its threat posture.

The value of Symantec Control Compliance Suite

Symantec Control Compliance Suite is a security compliance product that provides centralized and automated analysis of an organization's critical business applications and operating systems. It enables the organization to effectively manage business risks by identifying weaknesses and measuring compliance with security practices and regulations. Symantec Control Compliance Suite executes a variety of detailed security checks to determine compliance with an organization's security policies and provides specific templates for Sarbanes-Oxley, GLBA, HIPAA, Basel II, NERC, and FISMA (NIST 800-53) regulations, as well as for the SANS Top 20, COBIT, and ISO 17799 industry standards.

Through its reporting capability, Symantec Control Compliance Suite enables the organization to understand the critical components of its security posture by analyzing compliance across the entire organization, down to the region or office level or for specific systems. The product also helps the organization identify trends to measure progress and improve planning and prioritization. In addition, once problems are detected, the Symantec Control Compliance Suite provides more than 800 different remediation capabilities to rectify these deviations.

Segregation of duties

As noted previously, it is critical for the organization to enforce segregation of duties by performing testing of controls and providing robust reporting. In distributed environments, users with similar roles often have different permissions for each system to which they have access. These differences in access rights often lead to segregation of duties issues, which have an impact on the effectiveness of internal controls. In these cases, leveraging Symantec Control Compliance Suite to measure compliance with business rules for user access can allow an organization to identify and mitigate these issues quickly.

Symantec Control Compliance Suite is specifically designed to test technical controls. By using its templates for specific server configurations or regulatory requirements and customizing its own templates according to corporate policy, the organization can test the compliance level of numerous systems using a systematic and efficient method. This testing can include not only configuration settings, but also password strength, patch levels, dormant or unused accounts, and additional controls not viewable through native tools.

Creating scalable, repeatable, and sustainable infrastructure controls assessments

Further, Symantec Control Compliance Suite can be configured to perform testing automatically according to predetermined schedules that coincide with reporting requirements, system and application release dates, and scheduled maintenance windows. This flexibility allows an organization to view, track, and act upon a variety of changes to the environment.

The final component, reporting, details the way in which the organization can convert raw data into relevant, actionable, and timely information. The organization can author its own reports or select from a stable of predefined reports that can be accessed through a Web portal. These reports allow technical administrators to quickly identify items for remediation and changes investigation while allowing technical managers to allocate resources and set priorities. Executive management can obtain additional reports that provide a view of overall compliance metrics and measurements, as well as enterprisewide trending information.

Configuration management

Designed as an enterprise tool, Symantec Control Compliance Suite allows the organization to view and report data with a multitude of configuration options, as detailed throughout this document. This data allows the organization to understand and therefore control the technical configurations of its operating systems, databases, and applications. For example, by using predefined templates for Web servers, modifications can be made easily to accommodate externally facing servers (which require a higher degree of control) and intranet servers (which may not be business critical).

These modified templates allow an organization to test and report variances from approved configurations. If there are items that are out of control, they can be identified quickly and appropriate measures can be taken. Conversely, by identifying variances in configurations, an organization may determine that there is unnecessary complexity that can be eliminated, thereby reducing maintenance costs and overall risk.

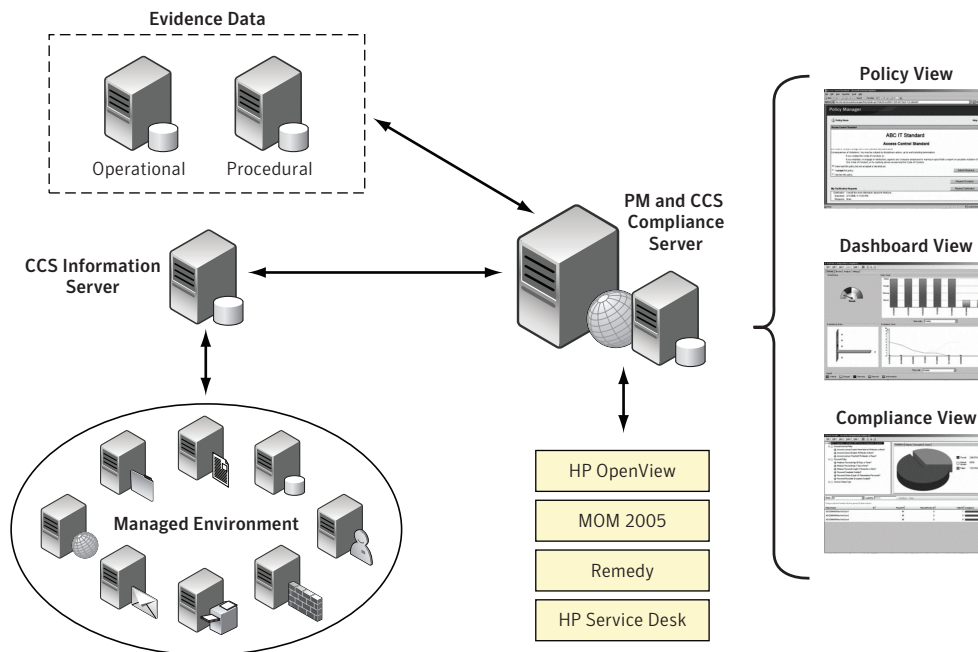


Figure 2. Symantec provides a fully integrated stack for policy compliance, minimizing total investment in infrastructure, while allowing a modular approach to get started quickly.

Resource management

Resource management ensures that users can only access those resources to which they are entitled. While Symantec Control Compliance Suite does not provide an enforcement capability, it does provide the ability to view system- and application-level access control lists, compare those lists to known values, and report on variances.

Since organizations already create access lists to enable and restrict access to files, folders, databases, mailboxes, and other securable objects, it is only necessary to tell Symantec Control Compliance Suite what these lists should contain. After that, the organization can view reports to determine whether additional users have been granted access to those resources or whether authorized users have been removed. This ability provides an organization with an additional layer of access control for information assets.

Integration with Symantec Bindview Policy Manager

Symantec Control Compliance Suite provides the leading solution for assessment of infrastructure controls against best-practice standards. But overall IT compliance requires more than infrastructure controls assessments. The organization must also assess the controls that relate to the operations of its environments and the procedures in place that cannot be programmatically assessed.

To unify these three kinds of control assessments, Symantec Control Compliance Suite integrates with Symantec Bindview Policy Manager. Symantec Bindview Policy Manager allows organizations to create human-readable policies that can be distributed to target audiences via the Web for sign-off and acceptance tracking. Evidence of compliance with these policies, as it relates to infrastructure activities, can be collected from the Symantec Control Compliance Suite. In addition, Symantec Bindview Policy Manager provides native facilities to gather procedural and operational control data. Together, these two products provide organizations with the ability to unify compliance across all components of IT into a single interface and back end.

Conclusion

To meet the increasingly complex requirements of internal and external constituents, an organization must implement processes, technologies, and other safeguards to protect critical data. Further, it must implement appropriate controls and develop a reporting strategy to demonstrate that these safeguards are in place, are regularly reviewed, and are working as expected.

An organization cannot create security compliance programs that demonstrate compliance without a clear strategy, well-defined roles and responsibilities, accountability, measurable processes, and effective technologies. Symantec Control Compliance Suite is one part of such a holistic solution.

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 and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Active Directory, Outlook, and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
9/06 10745926