

## WHITE PAPER

---

# Using Security Compliance Software to Improve Business Efficiency and Reduce Costs

Sponsored by: Symantec Corporation

---

Charles J. Kolodgy

Gerry Pintel

Rose Ryan, J.D.

June 2006

## IDC OPINION

Information is the lifeblood of the digital world. It is being collected at an ever-increasing rate, yet its protection and management leave a lot to be desired.

Governments worldwide are demanding, via legislation and regulation, that firms secure corporate and customer information and maintain integrity. Enterprises struggle to comply with the onslaught of new and expanding regulations. They are buried beneath the challenges of translating new policy rules to auditable controls, wading through the tools, data, and handling manual remediation processes.

Maintaining compliance is crucial for many enterprises, but it is an expensive endeavor. However, compliance may not be as costly as many enterprises envision. IDC believes the proper development of strong security policy and practices, combined with the deployment of an IT control architecture focused on compliance, may help enterprises, particularly those subjected to multiple regulations, reduce the overall total cost of compliance. Through the utilization of good IT control architecture, strong policies, and a technology solution capable of managing, maintaining, and reporting on the status of enterprise compliance, enterprises could significantly reduce the number of man-days required for supporting the compliance system.

## METHODOLOGY

This white paper was written in the summer of 2005 and updated in the spring of 2006. Based on historical and current research, IDC talked to customers and vendors affected by information and data laws in the United States, Canada, and Europe.

To reflect customer opinions, IDC conducted in-depth interviews with executives familiar with different regulatory compliance issues. IDC interviewed many different sized firms, from several different industries, focused on implementing solutions specifically designed for regulatory compliance. In these open-ended discussions, we listened to customers' external business concerns, internal organization problems, and solutions to address current and future governmental regulations. IDC focused this white paper on the enterprise customer's need to understand the cost and impact of regulatory compliance.

This IDC white paper:

- Illustrates the different cost elements in implementing a solution for complying with regulations
- Offers "best-practices" solutions with a corresponding technology feature set

## IN THIS WHITE PAPER

In this IDC white paper, we analyze the cost of complying with increasing numbers of governmental regulations. Certain regulations are discussed along with cost reduction strategies. Symantec's security solutions are cited as examples of how an enterprise can reduce its overall costs and still meet regulatory requirements with packaged solutions. Finally, we recommend strategies for implementing packaged compliance solutions.

## SITUATION OVERVIEW

### Defining the Compliance Problem

The Internet and increasing numbers of interconnected electronic systems brought about the easy sharing and collection of information of all types. Corporate scandals, such as those involving Enron, Tyco, Adelphia, and Eli Lilly, and the recent losses of personal records by Bank of America and CitiGroup highlight concerns voiced about the accuracy, integrity, and protection of corporate and personal data. As a result, legislators around the world are responding to the failures of governance, and a steady rise in identity thefts, with waves of new and expanded regulations. Table 1 lists legislation introduced in 2005.

**TABLE 1**

#### Legislation Introduced in 2005

Date Introduced	Bill No.	Bill Name	Original Sponsor	Purpose
March 3	H.R. 1069	Notification of Risk to Personal Data Act	Rep. Bean (IL 8)	Requires that consumers be notified when the security of their information is breached.
March 3	S. 500/H.R. 1080	Information Protection and Security Act	Sen. Nelson (FL)/ Rep. Markey (MA 7)	Directs the FTC to promulgate rules that set standards for information brokers, and then to report back to Congress.
April 11	S.751	Notification of Risk to Personal Data Act	Sen. Feinstein (CA)	Requires notification to consumers in event of unauthorized access to sensitive personal information.

**TABLE 1**

## Legislation Introduced in 2005

Date Introduced	Bill No.	Bill Name	Original Sponsor	Purpose
April 12	S.768	Comprehensive Identity Theft Prevention Act	Sen. Schumer (NY) and Sen. Nelson (FL)	Requires notice of security breaches, imposes obligations on data merchants to keep information secure, and restricts the use, sale, and posting of social security numbers as part of a comprehensive privacy and anti-ID theft measure.
29-Sept-05	s.1789	Personal Data Privacy and Security Act of 2005	Sen. Specter (PA)	To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

Source: IDC, Symantec 2006

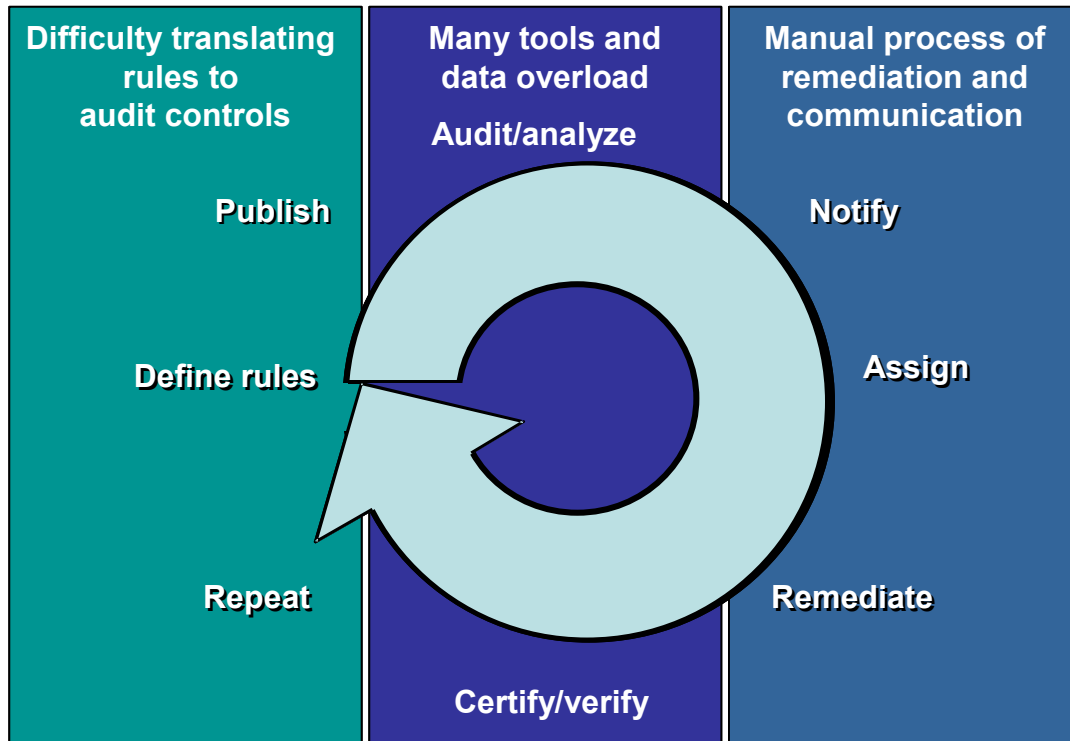
Because corporate and individual identity fraud continues to grow at a significant rate, often aided by easy access to personal data, regulators are not likely to relax their efforts for some time to come. Enterprises, therefore, remain awash in a sea of expanding regulations, with little hope the situation will improve. Complying with these regulations can be a significant cost to the enterprise, especially if the organization has multiple global locations or does business globally, because the organization will likely be subject to multiple regulations, thereby increasing the complexity, and thus the cost, of compliance.

### Common Compliance Pains

Enterprises are finding that implementing new regulatory policies and procedures in an automated and efficient manner is very challenging. The effort of translating the policy into actual technical controls and triggers is complicated and cumbersome. There are too many tools and too much data for them to process efficiently, and often much time is spent bringing these disparate elements together to analyze the results. Many of the enterprises' compliance processes, system remediation, and communications are managed manually. This complicates the issues and significantly increases the risk of error or compliance exposure. All of these troubles lead to significant pain and suffering for enterprises in dealing with their regulatory requirements. Figure 1 shows where the pains affect an organization's overall compliance life cycle.

**FIGURE 1**

Compliance Pains



Source: IDC, 2006

Many enterprises are subject to multiple regulations, which adds fuel to the fire. The basics of much regulatory reporting are the same, but managing the details is a complex problem. The keys are to find overlaps, to be able to reuse the data across multiple reports, and to manage the delivery of compliance data to regulatory bodies. Not only does the enterprise have to figure out how much security to apply and when, but now it also has to worry about which governmental body requires proof of compliance. IDC believes that while the multiple regulations situation does create broad challenges for the enterprise, there remains much leverage across regulations, making compliance less overwhelming and costly for those that can manage the compliance process. For instance, applying a solid security policy based on ISO17799 or a similar recognized and accepted security framework enables the enterprise to utilize one set of policy rules to manage its entire compliance infrastructure. Consequently, the centralized control of the monitoring, management, and reporting systems required for fulfillment of multiple regulation requirements will definitely reduce the effort required and, therefore, the cost to the enterprise.

## The Cost of Being Compliant

Deployment costs for new compliance technologies range from tens of thousands to tens of millions of dollars. At the lower end of the spectrum are enterprises that simply need to meet compliance requirements. Additional business efficiencies are not a top priority. At the higher end, tens of millions of dollars are required for those enterprises replacing entire infrastructures to cover regulatory exposures. At the same time, this class of enterprise often seeks significant business value from those investments. But it is the manual, labor-intensive nature of handling compliance challenges that drives up compliance-related costs. The time spent translating policy into auditable processes, sorting through and integrating the plethora of tools and data, and managing by hand the remediation and communication, represents a significant cost to the enterprise. These manual "gaps" are costing the enterprise too much money. While it is difficult to put the cost of the gaps into dollars, Table 2 provides some estimates of the cost of "time" to the enterprise. These estimates are based on real Sarbanes-Oxley, HIPAA, and GLBA compliance activities of midmarket companies, and they also apply to governmental agencies seeking FISMA compliance.

The IT-related activities clearly require a much higher amount of effort and time than the non-IT-related activities. When you add up the number of IT-related tasks in implementing compliance, they account for only about one in five, or 20%, of all tasks. But when compared with the man-days required to accomplish IT tasks versus non-IT tasks, the vast majority of the time involved in compliance (80%) is spent on IT-related tasks, such as evaluating and running IT controls and remediating problems. Therefore, if the effort required to complete the IT activities could be reduced, the enterprise has the opportunity to realize significant cost savings. 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.

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.

**TABLE 2**

IT and Non-IT Regulatory-Related Costs in Man-Days

Type	Tasks	Frequency/ Year	Cost (Days)	Total Cost/Year (Days)
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

**TABLE 2**

## IT and Non-IT Regulatory-Related Costs in Man-Days

Type	Tasks	Frequency/ Year	Cost (Days)	Total Cost/Year (Days)
	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		10	40
	Non-IT-related total man-days			295
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
	IT-related total man-days			924

Source: IDC and Symantec, 2006

As the saying goes, time is money (refer back to Table 2). Table 3 provides estimated costs associated with paying for the compliance tasks. IDC offers up three examples: professional services, internal manual, and internal automated.

Costs for each man-day are estimated, and individual situations will vary, but they should all be relative to each other. As illustrated in Table 3, a midmarket enterprise could be expected to spend over \$2 million to completely outsource the compliance operation during the first year. If it did the tasks internally, the costs in manpower would be around \$600,000 the first year. However, what can't be calculated in this figure are the opportunities lost because staff involved in compliance were not available for other activities. The first-year cost for the use of an automated system is around \$400,000. However, once the software is up and running, the cost is nominal because the system requires only software maintenance. Over a three-year period, a

software solution can cost up to 90% less than outsourcing and half of a manual process handled internally.

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

The examples provided in Tables 2 and 3 can be used to create enterprise-specific baselines that illustrate all of the tasks required to meet a specific regulatory requirement and the time required to complete them, as well as different costing options.

Note that estimated levels of effort for tasks and rates applied in these tables may vary considerably depending on the external and internal costs of a specific compliance project.

<b>TABLE 3</b>						
Estimated Costs to Meet Compliance (Professional Services, Internal Manual, Internal Automated)						
Task Group	Professional Services Rate	Cost (\$)	Internal Manual Rate	Cost	Internal Automated Rate	Cost (\$)
<b>Year 1</b>						
Non-IT related	296 man-days at \$2,000/day	592,000	296 man-days at \$500/day	148,000	296 man-days at \$500/day	148,000
IT related	924 man-days at \$2,000/day	1,848,000	924 man-days at \$500/day	462,000	\$200,000 software: 100 man-days at \$500/day	250,000
<b>Total</b>		<b>2,440,000</b>		<b>610,000</b>		<b>398,000</b>
<b>Year 2</b>						
Non-IT related	191 man-days at \$2000/day	592,000	191 man-days at \$500/day	148,000	191 man-days at \$500/day	148,000
IT related	924 Man days at \$2000/day	1,848,000	924 Man days at \$500/day	462,000	\$30,000 maintenance 1 employee at \$75,000	80,000
<b>Total</b>		<b>2,440,000</b>		<b>610,000</b>		<b>228,000</b>
<b>Year 3</b>						
Non-IT related	191 man-days at \$2000/day	592,000	191 man-days at \$500/day	148,000	191 man-days at \$500/day	148,000

**TABLE 3**

Estimated Costs to Meet Compliance (Professional Services, Internal Manual, Internal Automated)

Task Group	Professional Services Rate	Cost (\$)	Internal Manual Rate	Cost	Internal Automated Rate	Cost (\$)
IT related	924 man-days at \$2000/day	1,848,000	924 man-days at \$500/day	462,000	\$30,000 maintenance 1 employee at \$75,000	80,000
Total		2,440,000		610,000		228,000
3 -year Total		7,320,000		1,830,000		854,000

Source: Symantec, 2006

### Deciding to Invest in Compliance

The cost of compliance is so significant to enterprises that many will not be able to get any expenditure approved without solid proof of the return on investment (ROI). A recent IDC survey of enterprises revealed that technology investments are being strictly watched and contained to solutions that can easily provide significant value or added efficiencies to the organization. For instance, one such enterprise has no intention of increasing its spending on compliance-related activities, yet it is still considering a one-off SOX-compliant application because compliance must be tested continuously. In this case, it is clearly more efficient for this enterprise to install an application/database to ensure compliance going forward — even if it does not increase the overall budget or spending specifically allocated to compliance.

On the other hand, a few companies state they don't have any trouble receiving the funding they need for compliance. As one respondent reports, "All I have to say to the CFO is, 'By the way, the sanction for a breach is [a] \$250,000 [fine] and a year in jail!' He envisions himself with handcuffs on the cover of the *Daily News*, and he says that I can have the money I need!" But still this respondent capitulates, "It helps make the bosses happier if you can say to them that not only will this keep you out of jail, but it will have a good effect on our ability to provide this or that."

### In-House/Services Engagements Versus Packaged Solutions

Infrastructure to help reduce costs of compliance may be deployed in many different ways. However, the "many" can be boiled down to two broad approaches — deploying an in-house/services engagement custom solution or an "off-the-shelf" packaged solution. Each approach has advantages and drawbacks, but when cost alone is examined, the custom solution will cost more than the packaged solution.

Custom solutions are often subject to the multiples that systems integrators and consultants charge. Whether organizations develop the solution in-house or fully outsource it, the custom solution comes with a much greater expenditure of time, effort, and, consequently, money. The packaged solution, however, is ready for use "right out of the box," although it is likely a small services expense is required for integrating existing systems. Another complication associated with a custom solution is the hidden cost of upgrades. Often, even after the solution is in place and running, there are still large maintenance and upgrade costs. Many of these costs are hidden from view and may catch the organization unaware. Packaged solutions, such as the solution offered by Symantec, have an easily identifiable upgrade cost, which is still likely to be much less than the custom solution.

In the end, it is total cost of ownership that is the most important factor (after compliance itself, of course) for many enterprises. Packaged solutions may provide a much bigger bang for the buck. Only an in-depth review of business requirements and needs will reveal the best solution for the enterprise.

## FINDING THE RIGHT SOLUTION

In addition to cost reduction, enterprises want repeatable and internally controlled approaches to security and compliance. They are not interested in being subject to the vagaries of accounting firms' interpretations of audit firm results. Therefore, it is in the enterprises' best interests to build a secure infrastructure for regulatory compliance clearly showing their status and any required responses. Additionally, funds spent on complying with regulations may address other business needs, such as managing capital and/or operational costs. Before selecting a solution, the enterprise should take the time to see what other business needs may be fulfilled with the compliance infrastructure, thus lowering the total cost of ownership for the enterprise.

In calculating the long-term costs of regulatory compliance, the enterprise may discover that finding benchmarks is difficult because the needed infrastructure and services for compliance vary widely, depending on the particular situation of the enterprise. In general, an enterprise can expect higher cost in the first year than in subsequent years as the overall effort of complying is initially expensive in terms of hardware, software, and services bought — and also in the number of man-hours used by internal staff to deploy infrastructure and educate users in the use of the compliance system. Several companies IDC interviewed stated they were struggling with the number of employees focused on compliance, and in some cases, more than half of the IT staff was pulled off regularly scheduled projects and duties and redirected to support the compliance effort. The looming deadlines of compliance forced some enterprises to put aside other business and IT-related projects or hire more staff. The reassignment (or increase) of staff to compliance-related activities is in reality a detriment because of the internal opportunity cost of people not working on other projects.

Still, when the costs of compliance are being assessed, it is very important to note that operational costs of support, maintenance, upgrades, and services are usually significantly less per year than the first-year costs, but they continue in perpetuity.

In some cases, more than half of the IT staff was pulled off regularly scheduled projects and functions and redirected to support the compliance effort.

IDC believes a properly deployed packaged solution such as Symantec's should significantly reduce the cost of compliance through the reduction of time spent on manual tasks. With such a solution, employees could be redirected to (or remain on) other more strategic IT projects, and it may not be necessary to expand staff simply to stay abreast of the current compliance environment.

Eventually, the cost of supporting and maintaining the new solution in the enterprise overwhelms the initial cost. These post-fixed expenses benefit the most from automation and the reduction of manual effort and time. IDC believes a properly deployed packaged solution, such as Symantec's IT security compliance solution, should significantly reduce the cost of compliance through the reduction of time spent on manual tasks. With such a solution, employees could be redirected to (or remain on) other more strategic IT projects, and it may not be necessary to expand staff simply to stay abreast of the current compliance environment.

While there are many ways of reducing the costs of compliance, the use of technology to automate and consolidate many manual activities can significantly reduce the amount of time and dollars spent on complying with the different regulations. For some medium-sized firms that have trouble finding or affording auditors and consultants, the idea of being able to deploy technology that will address and monitor many of their compliance concerns without significant overhead or ongoing costs is useful indeed.

## **FUTURE OUTLOOK**

From an IT perspective, the key to compliance is the documentation, monitoring, and management of compliance control architecture. The architecture contains operational policy and technical controls aligned to business and regulatory requirements. It also establishes accountability, responsibility, and risk management principles ultimately mapped to the specific controls. In developing a control architecture, enterprises should follow a recognized control framework, such as COSO, COBIT, or ISO17799. Adoption of such a framework simplifies communication and ultimately validates the controls with regulators and auditors. When choosing a compliance solution, the enterprise should ask a series of penetrating questions of the vendor to determine if the vendor's product will fit the enterprise's needs and requirements. To illustrate the mapping of questions to a solution, IDC has chosen Symantec's packaged solutions as an example.

---

## The Symantec Solution

Symantec offers a repeatable, documented way to ensure continuing and ongoing compliance for the enterprise. Its technology offers a way of automating and integrating many of the most manual processes with which enterprises struggle. Additionally, Symantec's solution maps the compliance regulations into actionable IT controls. The ability to reuse this mapping across regulations provides efficiencies for the whole process. Controls can also be deployed to reduce system vulnerabilities, ensure secure configurations, and audit user rights and access control assignments. Symantec experts also create the policies and rules that handle new yet just-passed regulations, such as those noted previously (refer back to Table 1). Proactive management of such regulations will be a source of future ROI for the users of Symantec's solution.

Symantec's IT security compliance solutions (which include Symantec™ BindView Policy Manager, Symantec™ Control Compliance Suite, and Symantec™ Security Information Manager, Symantec Network Access Control, and Symantec Enterprise Vault [see the Symantec Product Portfolio section in the Appendix]) demonstrate compliance across an enterprise in a cost-effective manner. Symantec provides a compliance control architecture that:

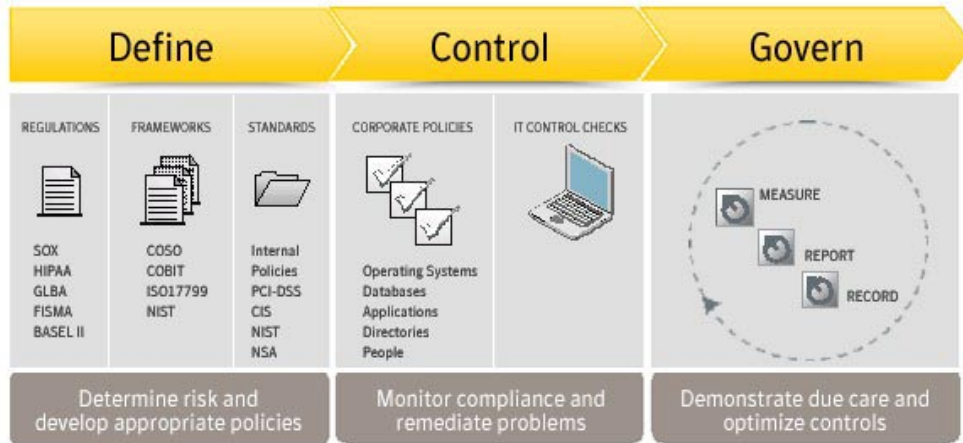
- Defines compliance through frameworks and standards mapped to regulations as well as:
  - Translates regulations into generally accepted frameworks and standards that provide the structure used to define operational policies and technical controls
  - Maps industry-accepted frameworks and standards to a set of technical controls and policies
  - Incorporates generally accepted best-practices standards, enabling you to leverage the same information used by your auditors when they validate compliance
- Implements compliance policies and IT controls based on accepted standards as well as:
  - Provides specific configuration settings mapped to IT policies that enable you to implement controls across a heterogeneous IT infrastructure
  - Provides the flexibility to customize operational policies and technical controls to meet specific company needs
  - Provides tools to help secure acknowledgement and agreement of personnel to security policies

- ☒ Demonstrates due care and sustains compliance as well as:
  - ☐ 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
  - ☐ Provides regulatory report packs that document and help you demonstrate compliance
  - ☐ Provides recommendations for remediating risks or holes in your security posture
- ☒ Demonstrates compliance due diligence in the following ways:
  - ☐ Assess IT risk — automatically discover systems and classify by risk
  - ☐ Monitor and correlate threats — correlate global threat intelligence with current activity to determine root cause
  - ☐ Prioritize remediation — workflow-based remediation capability with alerting and auditing
  - ☐ Audit activity — collect and store raw event logs for audit compliance
- ☒ Increases security, network availability, and regulatory compliance by enabling enterprises to:
  - ☐ Protect the network from dangerous endpoints by enforcing compliance on contact with the enterprise LAN, wireless network, and remote access services
  - ☐ Ensure the lowest total cost of ownership by managing integrated endpoint protection and network access control in one centralized architecture
  - ☐ Leverage existing network investments through integration with all major infrastructure vendors.
- ☒ Enhances electronic discovery and reduces storage costs by providing enterprises a flexible archiving framework to enable the discovery of content held within email, file systems, and collaborative environments that:
  - ☐ Ensures compliance with retention and discovery policies by acting as a secure repository for electronic information
  - ☐ Reduces the cost of content retrieval, recovery, and administration
  - ☐ Provides an "information warehouse" for corporate data that can be mined as a knowledge resource using built-in index and search technologies

The Symantec solution *helps* enterprises that are struggling to map regulations to IT compliance controls. Symantec logically structures the enterprise systems by applying a standard set of recognized policies to the regulations and, therefore, creates a best-practices framework that may be implemented across enterprises' infrastructures and people. Figure 2 shows Symantec's road map to compliance.

**FIGURE 2**

Symantec's Compliance Road Map



Source: IDC, 2006

To assist in its selection of the proper solution, the enterprise should make a list of questions addressing its needs and then line up the packaged solution's attributes against those questions to see if there is a fit. Table 4 lists questions an enterprise may ask a vendor and Symantec's IT Compliance features that answer these particular questions.

**TABLE 4**

Key Solution Selection Criteria and Symantec's IT Compliance Features

Selection Criteria	Symantec's IT Compliance Feature Response
<p><b>Scalability</b></p> <p>How is your solution deployed through the network?</p> <p>How does your solution scale? Can it deploy globally in large server farms and user environments?</p>	<p>The Security Information Manager (SIM) appliance is a self-contained unit, including integrated application and database software, so there are minimal deployment requirements. SIM aggregates logs from over 60 products with built-in agentless collectors. The Control Compliance Suite (CCS) scans systems by IP address from a central server, with no other deployment requirements.</p> <p>The Symantec solution scales to the needs of the enterprise. CCS can deploy globally across enterprise-grade environments, supporting environments of &gt;80,000 servers. A single SIM appliance can sustain over 3,000 events per second, with a sustained correlation in a clustered environment of 21,000 EPS.</p>
<p>What infrastructure is required to deploy your solution</p>	<p>CCS is an agentless solution that does not require any supporting infrastructure other than a dedicated server. No other agent software is required on scanned remote systems. SSIM is a self-</p>

**TABLE 4****Key Solution Selection Criteria and Symantec's IT Compliance Features**

Selection Criteria	Symantec's IT Compliance Feature Response
How reliable and accurate is your solution?	<p>contained appliance with no additional requirements, but optional direct attached or network attached storage may be used for archiving as desired.</p> <p>For CCS, It is significantly easier for enterprises to ensure the reliability of four data query engines versus 80,000 agents. SIM utilizes real-time feeds from Symantec's industry-leading Global Intelligence Network, and the largest vulnerability database, to ensure the reliability of security threat correlation, which is unique in the market.</p>
<b>Customizability/Flexibility</b>	
Does your solution interface with HR or ticketing/change systems?	Yes. bidirectional ticket and task management is available for Remedy ARS and Peregrine ServiceDesk. In addition, Symantec's solution is flexible enough to allow customization of the operational policies and technical controls to meet an enterprise's specific needs.
Will your solution populate databases?	Yes. SIM discovers critical assets and their associated vulnerabilities from Symantec and third-party vulnerability solutions as well as provides capabilities for classifying critical assets and their impact to CIA. CCS provides the results of system queries directly into its database.
Does your solution interface with operations management systems?	Yes. CCS integrates with HP OpenView Microsoft Operations Manager and Remedy to provide compliance, security and vulnerability data to the operations console.
<b>Regulatory Enforcement</b>	
Can your solution enforce segregation of duties?	Yes. The solution can establish administrative rules and approval mechanisms to ensure excessive rights are reduced and only authorized administrative changes are executed after garnering appropriate approvals (SOD).
Can your solution track and manage user access rights?	<p>Yes. The solution uses three methods for ensuring proper access control management that is required by most regulations:</p> <ul style="list-style-type: none"> <li>• Approval-based administration ensures and tracks authorization for any access control changes.</li> <li>• Entitlement reporting discovers effective rights in complex nested access-control environments.</li> <li>• Audit-log consolidation compiles and filters all administrative actions to provide comprehensive evidence.</li> </ul>
<b>Depth and Breadth</b>	
What platforms, directories, and applications does your solution support?	CCS supports Windows, Unix, Linux, NetWare, NDS/e-Directory, Active Directory SQL, Oracle, Exchange for compliance scanning;

**TABLE 4****Key Solution Selection Criteria and Symantec's IT Compliance Features**

Selection Criteria	Symantec's IT Compliance Feature Response
solution support?	SIM supports over 60 products (e.g., firewall, AV, IPS, VA scanners, etc.) from Symantec and third-party vendors for taking in data feeds.
Does your solution handle specific regulatory content?	CCS supports compliance assessment against several regulations (e.g., SOX, HIPAA, GLBA, FISMA, etc.), through frameworks and technical standards, to show it provides regulatory report packs that document and help demonstrate due diligence in compliance. SIM supports regulatory compliance by satisfying key IT control objectives, such as threat protection, incident response programs, log aggregation and forensics.
Does your solution provide forensics and reporting?	SIM provides tools for searching through raw event logs using a "Google-like" search capability and provides historical query and ad hoc reporting and auditing capabilities. CCS generally accepted best practices frameworks and standards enabling the enterprise to leverage the same information used by auditors when validating compliance.
What data presentation options are available?	<p>The solution has many levels of data presentation for different audiences in the IT environment. There are:</p> <ul style="list-style-type: none"> <li>• Raw asset-level views suited for discovery, classification, and association by policy.</li> <li>• Incident-based views that interpret the correlated data and prioritization of targets that are out-of-compliance with the security policy or assets that have been targeted by a threat.</li> <li>• Consolidated dashboard views that let you pinpoint issues.</li> <li>• Executive views that enable operations and other non-IT groups to quickly assess the current IT health.</li> <li>• Compliance-based views that interpret the data and align IT to policy and compliance goals.</li> </ul>
Does your solution measure up to NIST, COSO, ISO17799, ITIL, COBIT etc.?	SIM can help demonstrate compliance in the areas of assessment of IT risks, collection of raw event logs, monitoring, notification, reporting, and forensics for any standard or framework that the client chooses. CCS supports NIST, COSO, COBIT, and ISO 17799 for system compliance with framework requirements.

**TABLE 4****Key Solution Selection Criteria and Symantec's IT Compliance Features**

Selection Criteria	Symantec's IT Compliance Feature Response
<b>Support, Maintenance, and Upgrades</b>	
What response does your solution have to break outs?	Symantec Security Information Manager includes the Symantec Global Threat Network from Symantec™ DeepSight™ and automatically correlates threats from over 30,000 malicious IPs from the around the globe. Backed by Symantec Security Response labs and the Symantec Security Information Manager internal and external incident and ticket handling systems, it is well positioned to be the fastest Symantec Security Information Manager response solution in the marketplace today.
Does your solution operate off a sampling of the environment, or does it allow for analysis of the entire environment?	Yes, through the integration of Symantec™ Intelligence Network. In addition, the solution leverages the architecture and automation to analyze the entire environment to allow for remediation across the enterprise.
What sort of content advisor does your solution have?	The regulatory content is regularly updated and expanded to keep in step with industry standards. Vulnerabilities, exposures, malicious code, and safeguard content are included with SIM via real-time feeds and monthly content updates via LiveUpdate™.

Source: IDC, 2006

Many enterprise needs around the security aspects of compliance may in fact be met by a packaged solution such as Symantec's. Symantec's products offer enterprises the flexibility to choose the specific functionality they need without suffering the high cost of a custom solution. Symantec's software solutions combine best-practices knowledge with automated controls to demonstrate and sustain compliance at a reduced cost.

It is important for the enterprise to realize that with solutions such as Symantec's in place, the cost of compliance may not be as high as feared. Implementing processes and policies looking at each compliance element and responding to that specific gap or element with a more automated solution can help reduce the most costly of compliance elements — people's time. Symantec's solution will reduce the amount of time people have to spend on often menial and mind-numbing tasks and provide a secure and well-documented method of addressing the demands of compliance auditors.

Symantec's solution will reduce the amount of time people have to spend on often menial and mind-numbing tasks and provide a secure and well-documented method of addressing the demands of compliance auditors.

## **CHALLENGES/OPPORTUNITIES**

Many of the challenges in implementing compliance solutions are tied to the complexity of finding solutions that address the different regulations. Symantec's packaged solutions do address many challenges pertaining to regulatory compliance, although additional issues must be overcome.

A packaged solution may not simply be "plug and play" in the existing enterprise network. Despite the low requirement of customization, there remains a need to ensure proper integration into the enterprise's standing systems. To address such concerns, Symantec partners with several large systems integrators and provides its own professional services team.

While a packaged solution may provide a cost-efficient method of deploying a needed compliance solution, it may not, by nature, meet all the needs of the enterprise. Particularly if the enterprise has a need to gain additional business value from the solution, the packaged solution may be challenged to provide the specific value needed by the enterprise.

Custom solutions often come with embedded support services. A packaged solution may lack in the needed support and maintenance necessary to keep the environment continually secure and airtight. Symantec offers a full array of security compliance training and professional services capable of infusing knowledge and accelerating skill development. While perhaps not the same as a full-blown outsourced service, the services provided by Symantec will more than cover the services gap that enterprises perceive packaged solutions have.

Many companies do not know how to get started with compliance initiatives and therefore may not be positioned to benefit from packaged solutions. Symantec offers a starter kit that provides an ideal first step — especially when time and money are limited.

Overall, while there are many challenges to deploying a packaged compliance solution such as those provided by Symantec, the reality is that most of the challenges may be addressed quickly, easily, and cost-effectively.

## **CONCLUSION**

Containing the costs of responding to all the government requirements is becoming a very important focus for the enterprise. However, demonstrating proof and sustaining security compliance don't have to devastate the bottom line. Deploying an IT control architecture for automatically maintaining compliance requirements will significantly reduce the amount of time and energy spent on manually managing the many processes related to ensuring compliance. Additionally, more cost reduction may be found in the use of a sophisticated packaged solution, such as Symantec's offerings, instead of a wholly custom solution. By deploying software such as Symantec's, the enterprise can automate most of the manual tasks it needs to complete for IT compliance, thus reducing its total cost of compliance between 50–90% (refer back to Table 3).

## APPENDIX

### Brief Regulatory Descriptions

Table 5 provides brief descriptions of the SarbOx, HIPAA, PIPEDA, GLBA, EUPA, CA SB 1386/1950, Basel II, and FISMA regulations.

**TABLE 5**

#### Brief Descriptions of Selected Privacy Regulations

Regulation	Brief Description
SarbOx	Sarbanes-Oxley redesigned the accountability requirements for corporate governance officers, requiring CEO/CFOs to certify their company's financial results and be held personally accountable for the results. The penalties are now much more severe and carry both criminal and class action suit potential. Sarbanes-Oxley is aimed at preventing, or at the very least deterring, more corporate scandals such as MCI and WorldCom. As such, corporations will be accountable for their numbers and required to implement a series of internal audit and self-assessment tools to ensure compliance.
HIPAA	HIPAA regulates the protection, portability, and privacy of an individual's medical information. HIPAA impacts any organization that maintains health information as well as all of their partners and vendors. Medical information is highly sensitive and the potential for abuse of that data is extremely high. The act requires organizations to protect information from security violations and correct any problem as violations occur.
PIPEDA	Much like HIPAA, PIPEDA prohibits the collection, storage, and disclosure of personal information related to an individual without that person's explicit consent. Personal information is any factual or subjective information, recorded or not, about an identifiable individual. Provides the individual the right to know what is being collected and change the information if it is inaccurate. Interestingly enough, U.S. and U.K. businesses may also be bound by the rules protecting Canadian citizens' personal information.
GLBA	Specifically targeted at the financial industry, GLBA protects the personal non-public data of bank and financial institution customers from internal or external threats or hazards as well as the unauthorized use of said data.
EUPA	The EU Act focuses on ensuring that member states require the prohibition of collection of certain data, and provide for stringent protections for the data that is collected. This Act however, doesn't provide for any punitive measure for noncompliance. Rather it requires the member states to provide the punishments. It is applicable to all businesses regardless of industry, size, and shape.
CA SB 1386/1950	The CA SB 1386 bill applies to companies that do business in California — whether or not they have any physical locations in the state. Its main stipulation is that all businesses must disclose the breach of any personal and private information as it pertains to California residents. It contains no criminal or civil penalties, but does permit class action lawsuits. SB 1950 expands 1386 by requiring that all businesses in possession of California resident data provide reasonable security procedures and practices to protect the information and that they receive a contract from any third parties to which they share the personal and private information that stipulates the maintenance of reasonable security practices on the part of the third party.

**TABLE 5****Brief Descriptions of Selected Privacy Regulations**

Regulation	Brief Description
Basel II	The New Basel Capital Accord, known as Basel II, requires the improvement of risk and asset management in order to avoid financial mishap. All banking institutions are required to have the assets to offset any risks they have. This is represented through an 8% capital to risk aggregate ratio. First part of this compliance was that the data capture was due in 2004. By 2007, institutions must have three years of data on file. The requirement is ongoing and cannot be considered a one-off or annual review.
FISMA	The Federal Information Security Management Act of 2002 (FISMA) was enacted in 2002 in the United States. This Act was meant to address the weak computer and network security within federal government and affiliated parties through the mandate of annual audits. Previously cyber security was often neglected in the federal government, and many agencies received rather poor marks on their audits.

Source: IDC, 2006

## DEFINITIONS

### Symantec's Product Portfolio

Symantec has five primary products focused on particular enterprises' security compliance pain points:

- ☒ **Symantec™ BindView Policy Manager** automates the process of defining, documenting, and tracking user acceptance and promoting awareness of security policies to employees across the organization.
- ☒ **Symantec™ Control Compliance Suite** allows security and audit professionals to continuously measure and manage compliance of systems to regulations such as Sarbanes-Oxley.
- ☒ **Symantec Security Information Manager** enables IT to quickly and effectively identify, prioritize, and respond to critical incidents that impact the security and compliance of IT applications and services.
- ☒ **Symantec™ Network Access Control** increases security, network availability, and regulatory compliance by enabling enterprises to enforce security settings and software running on the hosts connected to their enterprise networks. Support for the widest variety of network equipment, access methods, and protocols in the industry helps organizations maximize ROI by eliminating ties to specific vendors.
- ☒ **Symantec™ Enterprise Vault** provides a flexible archiving framework to enable the discovery of content held within email, file system, and collaborative environments, while helping to reduce storage costs and simplifying management. Powerful search and discovery capabilities are complemented by specialized client applications for corporate governance, risk management, and legal protection.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.