Ptak, Noel & Associates

White Paper

Policy Compliance Checking: Making the Right Decisions

Abstract:
Today's Enterprises face an unprecedented challenge in mandated, managed oversight. This especially holds true when applied to financial data in terms of security, storage, management and manipulation. The ramifications, both legal and operational, of non-compliance with an increasing number of legislated mandates have raised concerns over how to choose and implement compliance management solutions. This paper summarizes the drivers behind these concerns. Using the Sarbanes-Oxley Act as an example, the product requirements for policy compliance management are introduced. The major issues surrounding product selection are discussed. The overview discusses the impact of enterprise security maturity and then moves on to the two major architectural approaches taken in providing compliance management tools. Product requirements are discussed and summarized. Symantec Enterprise Security Manager (ESM) serves as the basis for illustrating one vendor's approach to solution implementation.

Policy Compliance Checking: Making the Right Decisions

Table of Contents

Introduction

Enterprise security has moved significantly beyond the point of simply thinking and acting on concerns over the physical security of assets and equipment. Security managers can no longer afford to function in a siloed, bottoms-up approach – treating intrusion detection, virus and vulnerability management, and access control as related but independent specialties. Today enterprise security requires a broader view.

Over the past several years, the combination of intelligent, coordinated attacks and legislative mandates forced a radical change in enterprise security focus. Security must now encompass not merely the processes of physical protection and monitoring of assets, data, visitors and infrastructure but enterprise operational policies and their application. As a result of laws such as The Sarbanes-Oxley Act, HIPAA, the Basel II Capital Accord in EMEA and Gramm-Leach-Bliley, enterprise security of assets, data (in all forms), and the derived information receives special attention.

Enterprise security and Information Technology infrastructure has become a CEO-level and board room issue, not just a technology issue. These laws include a focus on corporate governance that transformed security into a major business concern. Unauthorized intrusion and e-based theft have become a vicious, global activity. Increasingly sophisticated threats combine with legislated accountability and control functions to drive enterprise efforts to implement new programs to create and enforce comprehensive security policies.

Implementation of any, let alone a comprehensive, security program represents a significant business decision. Any such program must be based on quantifiable, enterprise risk-benefit analysis. The success and appropriateness of an enterprise security policy will be determined by two factors:

1. An assessment of enterprise threats and vulnerability (and associated damage) to security attacks and intrusions to determine level of risk and justify expense, and
2. Compliance with enterprise policies in security plan implementation. Operationally, this means passing security audits and demonstrating due care in security practices to shareholders.

In this paper we will examine the challenges, solution requirements and issues associated with policy compliance management. Compliance management, for our purposes, includes policies that implement regulatory, industry and corporate mandates and standards. Sarbanes-Oxley is used as an example of current regulatory mandates. After discussing these topics, Symantec Enterprise Security Manager serves as an example of one vendor's approach to meeting the solution requirements. We will begin with a look at the forces behind the interest in compliance management.

The Day-to-Day Challenge

Policy Compliance – Standards and Mandates

Legislation and standards are the means by which an ordered society attempts to bring structure, order, and consistency to the messy and complex world of the competitive enterprise operating in the market. Standards, voluntary and mandated, in technology have been used to leverage the benefits realized from the application of technology through consistency – consistency in interface, function, and implementation. Standards ease comparisons among competing choices. Finally, standards also help to fulfill a watchdog

function by providing a consistency in assessing and reporting about enterprise activities. Such monitoring and reporting are aimed at protecting participants from misrepresentation, fraud and abuse. Standards, used in this way, describe protective criteria for collecting, storing, managing access and reporting on enterprise processes dealing with data and data manipulation.

The closing years of the twentieth century have seen an explosion in legislation concerned with enterprise oversight and governance. As IT moved to the center of enterprise operations, it provided a powerful tool for implementing and enforcing mandates aimed at protecting and reporting on corporate assets, information and infrastructure. Rules, recommended procedures and standards creation have become an industry in and of themselves. In addition, those mentioned earlier controlling laws and supporting bodies include: International Organization for Standardization (ISO), Common Criteria for IT Security Evaluation (ISO/IEC 15408), Information Security Forum (ISF), Process Control Security Requirements Forum (PCSRF), Statement on Auditing Standards (SAS70) No. 70, Committee of Sponsoring Organizations of the Treadway Commission (COSO), and so on. (Appendix 1 lists the most prominent.)

A major piece of today's IT resources used in enterprise security management involves tracking and reporting on efforts to comply with and support relevant standards body recommendations and satisfy legislated mandates. Information security consists of three main components: Confidentiality, Integrity and Availability. The first regulatory concerns were focused on data confidentiality, especially in the healthcare industry, producing the HIPAA legislation. Then the concerns turned to data integrity, addressed in the Sarbanes-Oxley Act.

In a typical enterprise, IT has significant operational involvement in the implementation of secure processes. Information Security administrators and auditors typically monitor the administration and compliance state of policies. This separation of duties between IT and Information Security Administration is essential. IT's goals focus on maximizing uptime and optimizing performance, not necessarily security, often viewed as intrusive. IT may also be responsible for providing the underlying business services which are being monitored.

Thus, IT will be intimately involved in the design and implementation of enterprise security programs. Programs which will usually include IT infrastructure assets as well as the tools and processes that implement the policies required for compliance with the various standards and mandates. Finally, security plan design and implementation will include policy compliance management – a top down management task for monitoring and reporting on the application of policies designed to assure compliance with mandated protections and procedures. Let's examine how an enterprise may structure its security plan.

Policy Compliance – Enterprise Maturity

Efforts aimed at complying with legislated operational and reporting mandates pose a dilemma for enterprises. Unless confidentiality and control constitute a basic part of their services such efforts distract from the fundamental task of a business to profitably deliver goods and services to customers. Successful enterprises must define and implement a security strategy and plan appropriate to their business operation in terms of its overall security vulnerability and mandated processes. Security measures must to map to business objectives. A balance has to be struck - too much effort and too many resources focused on security and compliance management wastes enterprise assets – resulting in upset investors.

Too little or misapplied security efforts can result in loss due to theft, fraud, or non-compliance with mandated actions – leaving both the firm and its executives subject to potentially enterprise-destroying losses, fines, sanctions, and even imprisonment. The approach taken in a security strategy depends on three things:

1. The business focus of the enterprise (which determines which and how much governance pressure apply as well as its level of vulnerability and risk – an office services firm functions has different risks than a medical records management firm.)
2. Enterprise size in terms of revenues, market share, etc. (which determines vulnerability and scrutiny– a family bakery has different vulnerability than an international food processor.)
3. Level of security maturity (determined by management level of experience and sophistication in understanding security costs, risks, vulnerabilities, and accountability – a brokerage firm will operate at a higher level of security maturity than a local auto body repair shop.)

Focus and size are obvious, but what is security maturity? Security maturity describes the level of enterprise operational thinking about security. The maturity levels ranging from least to most mature are shown in Figure 1. At Level 1 (the entry level), the focus is on reactive response to vulnerabilities; at Level 4 (the highest level) the focus is on having an integrated plan to comprehensively address all enterprise security challenges.

Note that enterprise size does not necessarily correlate to maturity; relatively small companies (a private bank) may operate at a very high maturity level. Different industries operate at different levels; for example, the financial industry is more mature than the transportation industry. We focus on Level 2 – Policy Compliance.

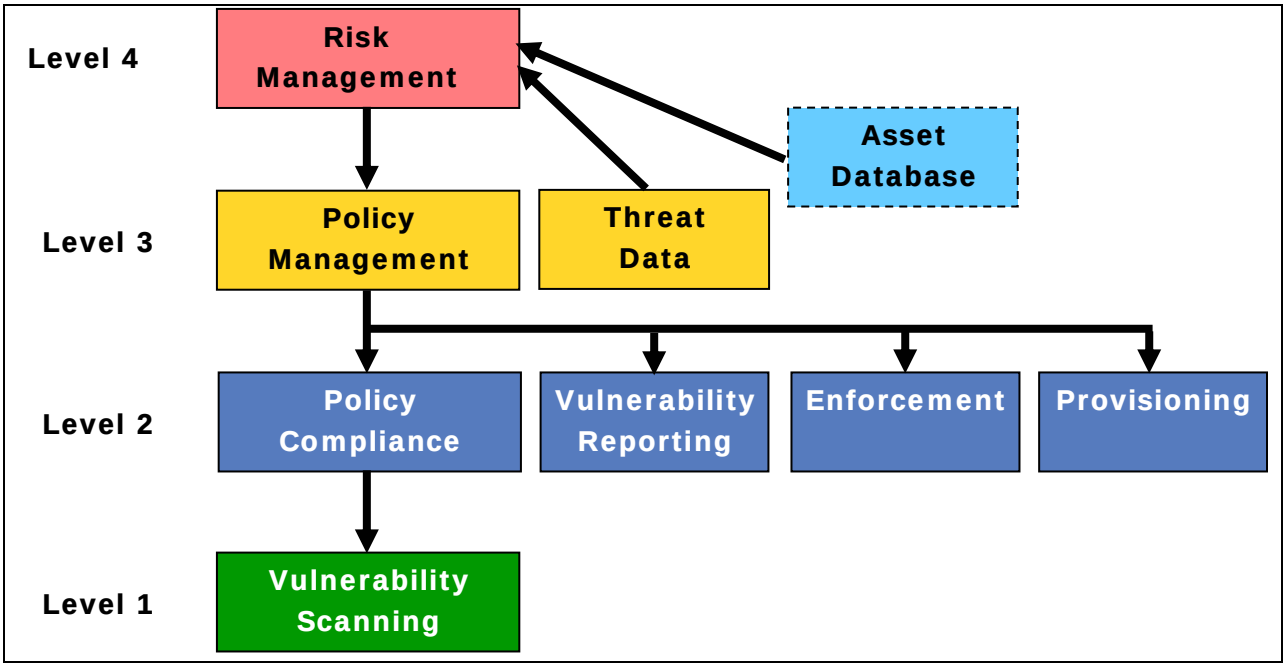


Figure 1 Levels of Security Maturity

Policy Compliance – Proactive Security

Security can be proactive or reactive. Proactive action will generally always be less expensive than reactive because it attempts to identify and eliminate threats before they cause damage or lost revenue.

1. Risk Analysis – comprehensive review relating and linking business objectives to assets, threats and vulnerabilities.
2. Policy Management – maintaining comprehensive policies for physical, logical and procedural security that encompass upper management support, regulations and standards, procedures, guidelines, practices and controls.
3. Policy Compliance Management – proactively assess and monitor mitigating controls across threat areas needed to assure enterprise systems and procedures comply with corporate policy and government mandated regulations
4. Vulnerability Assessment – structured analysis to identify vulnerabilities and develop a mitigation plan (bottoms up assessment of operations)
5. IDS/Firewall – monitoring and low-level protection against unauthorized intruders
6. Incident Management – react after a security breach or attempted breach has occurred

The first four levels proactively identify and respond to potential security problems. The last two levels tend to be reactive in nature. Thus, the enterprise response to security threats and mandates includes a considerable range of options and can take many forms. Some firms elect to wait and only react when actual incidents or security breaches occur. These plans make sense when the business cost of a security failure is low, probability of a threat occurrence is low, or the risk of a breach poses little threat to the health of the business. This approach is analogous to buying fire insurance after the house burns down.

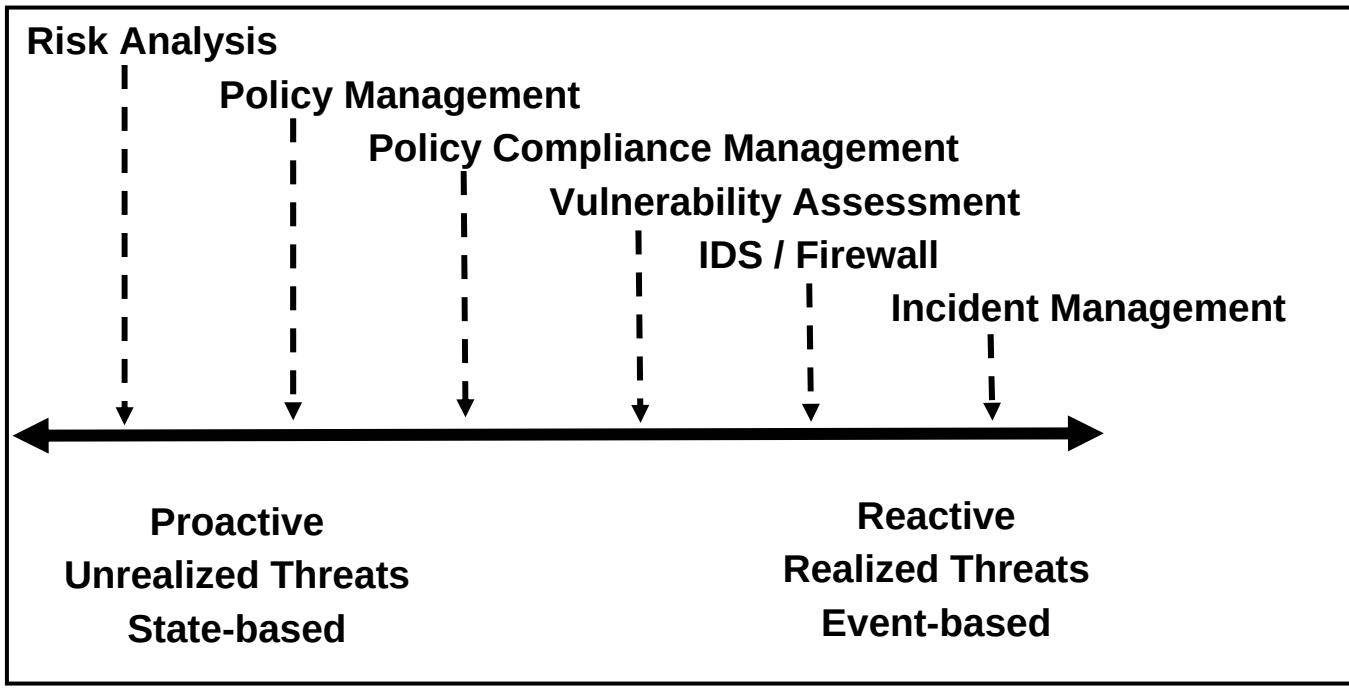


Figure 2 Proactive vs. Reactive Security

Security mature firms also tend to develop plans to operate proactively – to actively anticipate, seek out and avoid as much as possible potential problems and conflicts. Such proactive planning comes under the area of policy compliance management. Policy compliance management focuses on assessing enterprise systems and procedures to assure they are set up and operated in a manner that complies with enterprise policies and government mandated structures.

Both proactive and reactive security plans are necessary. Proactive security is like teaching someone to balance their checkbook. Reactive security is like teaching someone to manage bounced checks. Proactive security is generally less costly than reactive security. Let's see how a specific mandate, Sarbanes-Oxley, frames the problem.

Policy Compliance – Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 (SOA) concerns itself with the integrity of the financial reporting process for US publicly traded companies. It establishes operational guidelines in three areas of financial data management: configuration management, change management and resource management. SOA describes operational checks and reporting procedures to assure compliance with its guidelines. To further encourage compliance with its mandates, SOA further defines civil and criminal penalties for officers and outside auditors if financial information is not accurate and complete. In sections 404 and 302, SOA mandates annual and quarterly reports on the state of enterprise compliance with SOA mandates. Thus, the enterprise becomes accountable for operational activities to achieve and maintain compliance as well as its ability to monitor and report on the state of compliance with SOA mandates.

Sarbanes-Oxley describes a framework for building and reporting on a structure of best practices to manage and maintain enterprise financial data. SOA mandates policies that impact IT operational activities in three specific areas. The impact is seen in the requirements for operational management control and supporting reports that deal with IT infrastructure in terms of:

1. Controls Compliance (Configuration) Management – this policy focuses on the state of system configurations. System configurations and settings are monitored and maintained to assure they operate in a way that supports and enforces enterprise policies. Specifically the policies designed to assure compliance with and preservation of the states and levels of financial data control mandated by SOA. The implementation in the enterprise includes management report alerts to non-compliance with SOA requirements.
2. Change Management – monitoring, detecting and reporting changes to the IT systems (i.e. registry), file, network and operations infrastructure that can impact the system of controls implemented to assure compliance with SOA mandates. The implementation in the enterprise is to include management reports in order to meet disclosure requirements.
3. Resource Management – monitor the state of infrastructure resources used to maintain and manage financial data in compliance with SOA requirements. Monitor for activities and perform operational assessments to respond to identified risk, to assist in periodic assessment of administrative and technical controls that assist compliance with SOA mandates. Provide for the creation of reports reporting on and assessing the level of compliance and threats to compliance.

Translating these mandates into solution requirements depends upon the viewpoint taken of the infrastructure. For our purposes, Sarbanes-Oxley compliance can be viewed as a matter of conducting

and reporting the results of infrastructure and process audits. Let's examine audits and operational requirements that will meet SOA.

Audits: Implementing Sarbanes-Oxley

The implementation schema for Sarbanes-Oxley focuses on the ability to conduct an audit of enterprise processes and policies. Audits provide a disciplined, structured review of what an enterprise does to protect, store and manage its financial data. SOA provides a detailed description of what must be checked. It includes specifications that cover the frequency, content and recipients of reports describing actions taken to meet SOA mandates. The reporting must include a statement on the level of enterprise operating compliance with SOA. It does not specify how to perform the checks or how to create reports. It does specify report content and timing.

Only three of over 60 sections in the Sarbanes-Oxley Act, relate to security: Section 302, 404 and 409. Section 404 focuses specifically on internal controls. To be compliant, internal controls must be implemented in accordance with a generally accepted framework, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (see Figure 3 below). Section 404 of SOA affects managers and departments throughout the enterprise. SOA requires them to submit annual reports which document the effectiveness of internal controls and specific financial reporting.

Reporting requirements include:

1. An internal control report from business managers
2. An assessment of the effectiveness of internal controls
3. A report for auditors

SOA applies to data protection processes in both hosted (primarily mainframe) and distributed (networked) environments. The two architectures have in-built, fundamentally different operating philosophies. Hosted assumes privileged access while distributed generally assume non-privileged access. These philosophies govern control and access functions that directly impact how and what can be done in terms of monitoring, managing and controlling resident data. Either or both architectures can be used in the collection, management and manipulation of financial data. There are benefits and drawbacks to each. The differences become apparent in the functioning of privileged and non-privileged audit implementations. The information security manager responsible for conducting compliance audits needs to understand the differences and solution implications inherent in each of these environments.

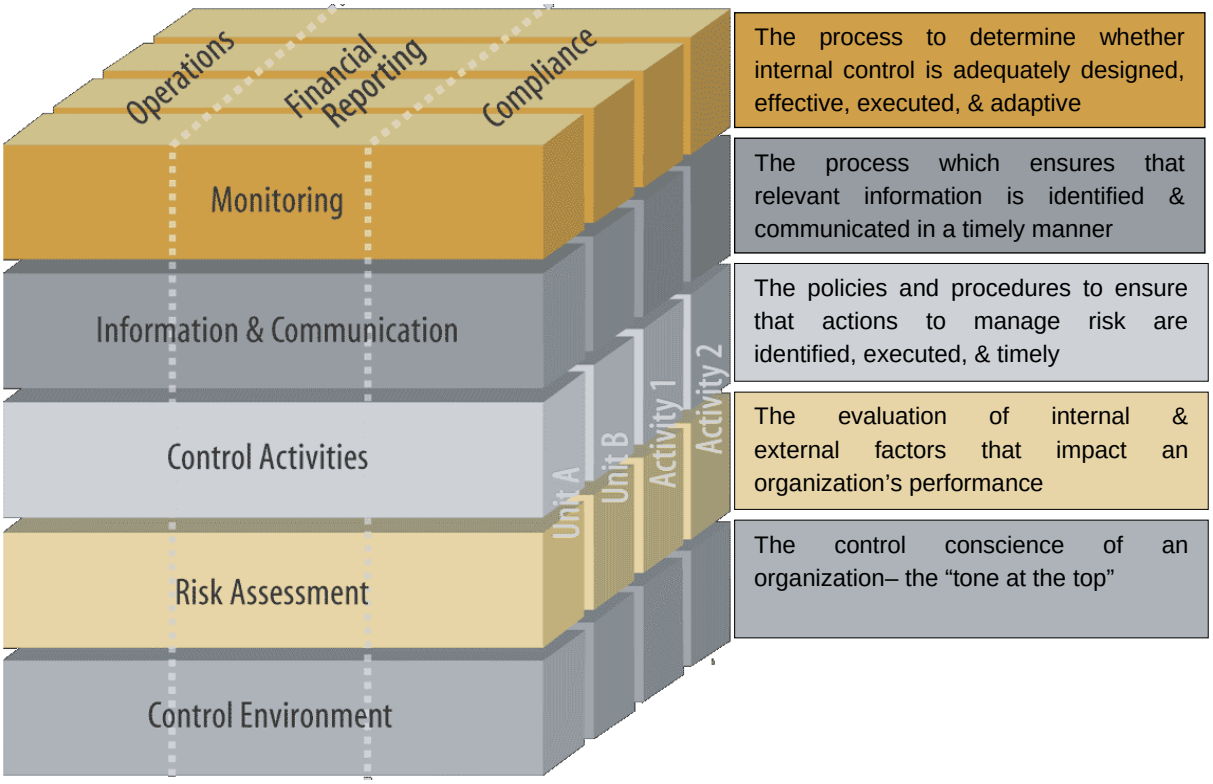


Figure 3 COSO Integrated Control Framework for SOA Control

(Source: COSO, www.coso.org, and Deloitte)

Privileged Access Auditing

Privileged access auditing assumes system privilege level access can be granted to all systems being assessed (root level). Auditors with privileged access have available tools with much more power and capability to access accurate data. Once authorized, the auditor has open read-only access to any part of the infrastructure. Privileged access environments are the most efficient and effective for audit purposes.

Because multiple applications and data reside on the same system, privileged environments will typically have direct access between monitoring applications and data about the systems and processes being audited. Agents are not needed to collect, store and pre-process data to transmit information or event data to another controller. Agents with their administrative overhead and potential for management problems are generally used only when no other acceptable option exists.

Hosted environments are typically set up to support privileged access auditing. Remote or networked systems may or may not be set up for privileged access audits.

The major drawbacks for a hosted architecture include:

1. Administrative, functional or logistic considerations may make a hosted system impossible
2. Hosted systems are less likely to be dedicated so performance may be lower
3. They are potentially a single-point of failure

Non-privileged Access Auditing

Non-privileged access auditing systems operate with limitations on data, functions, and controls. These usually appear in open environments, where access by users (including both naive and malicious users) is less controlled and controllable. There exists a higher risk of malicious and unauthorized access and use of systems and contents. The auditor has much less system capacity and functionality to work with in monitoring and assessing what is happening on the system. In the same way, security and control functions operating on the system will be limited.

Most remote, networked systems are set up as non-privileged auditing systems. Such systems and devices are not expected to act as expansive command and control systems.

Even if privileged access is possible, the range of functions that can be exercised and data collected is normally quite limited compared to hosted systems. Agents and scripts can be used to collect data and perform local processing to acquire and feedback audit results.

Some of the drawbacks to distributed systems include:

1. Potentially greater security risk
2. Limited access to data
3. Limited operational and control functionality

Table 1 below provides a summary of the advantages and drawbacks to be considered when selecting privileged versus non-privileged access auditing environments.

	Advantages	Disadvantages
Privileged Access Audit		
Host-based	Provide the highest level of security	Potentially a single-point of failure
	Unhindered access to lots of data and information	Performance impacted by sharing resources
	Access to more comprehensive and accurate information	Logistics, administration or structure may prevent use
	More efficient operation	Initial operational costs to deploy and upgrade agents
	More control	Limited platform support from vendor solutions
	Less network bandwidth utilization	Politics of system ownership and use can complicate data access and use
	More scalable and flexible	Tools usually more expensive than network-based solutions
	More CPU friendly (can run as low priority processes)	
	More efficient in WAN environments	
Agentless	Less administrative overhead	Difficult to provide privileged access for all platforms and devices due to non-standard authentication protocols (PDC vs. RPCs)
	Lower system resource load	Less secure if passwords are passed across the wire
	Less management complexity	Central storage of all network passwords used for authentication (single stop shopping for hackers)
	Easier to deploy	More network bandwidth utilization
	Best way to audit network devices such as routers, printers and wireless access points	Full access is not always attainable
	Tools usually less expensive than host-based solutions	
Non-privileged Access Audit		
Network-based	May be the only way to collect data	Limited information may lead to wrong conclusions (false positives and false negatives)
	Outside looking in or “hacker’s eye” view	Limited in auditing functions/capabilities
	Less administrative overhead	More network bandwidth utilization
	Less management complexity	Limited access (blocked by firewalls)
	Easier to deploy	Better suited for vulnerability assessment than for policy compliance audits
	Able to audit network devices such as routers, printers and wireless access points	Inefficient if used over slow WANs
	Tools usually less expensive than host-based solutions	
Scripts	Expanded command functions	Maintenance/update
	Automatic execution	Typically less accurate or complete
	More politically acceptable if agent-based solutions are prohibited	Less secure since audit results are often transferred in clear text
	User extensible (can add custom checks)	Potential configuration control issues (IT may alter)
	Scripts are more standard than proprietary vendor tools	

Table 1 Privileged Access Audits vs. Non-privileged Access Audits

Most enterprises today operate with a mixture of hosted and distributed systems. Any viable policy compliance management product will have to support both modes of operation along with privileged and non-privileged modes of auditing.

In general, privileged access is preferred to non-privileged access due to accuracy of the data collected and therefore the results. Host-based is more difficult to deploy, but easier to manage and is less resource intensive once deployed. Since host-based solutions cannot be installed onto many network devices, such as routers, hubs, firewalls (voids warranty), some appliances, network printers, and wireless access points, both host and network technology will usually be required to perform a holistic policy compliance audit. Network-based auditing tools are often preferred to audit user workstations due to the sheer number of them deployed. Host-based tools are preferred to audit mission-critical servers such as database and ecommerce servers.

Let's examine Symantec's Enterprise Security Manager to see how one vendor addresses policy compliance checking.

Symantec Enterprise Security Manager

Symantec Enterprise Security Manager (ESM) with Sarbanes-Oxley Act preconfigured policies uses a policy-based approach to monitor, assess and report compliance to key portions of the Act. ESM focuses on providing support to enterprises as they:

1. Engage in ongoing activities to achieve and maintain overall SOA compliance
2. Provides change management by monitoring baseline snapshots per SOA requirements
3. Develop audit and examination reports on the current state of their compliance efforts

Enterprises balance action with monitoring and reporting activities in order to meet the mandates as specified in Section 404 of SOA. Symantec defines the creation, implementation and application of policies designed to support the enterprise in on-going compliance efforts. Specific policies are presented in three areas which map to the Sarbanes-Oxley concerns. These policies are:

1. Controls Compliance – to report on system-wide configuration settings related to how effective internal controls are and to address the concerns of the controls compliance management portion of SOA.
2. Resource Review – to report and provide information about critical systems resources for the resource management section of SOA.
3. Change Notification – to identify changes to systems resources and other parameters concerned with the effectiveness of internal controls for the change management sections of SOA.

Symantec ESM policies are structured to assess compliance with many of the components of internal control as specified in COSO and to comply with the control objectives as published by CobiT. Let's step through the policies.

Controls Compliance Checks

Bi-weekly Symantec ESM policy audits are recommended in order to report and assess if the actual operating environment is in compliance with the desired state of control. The policy also monitors the state of control for compliance with the desired state. Thousands of audit checks are provided for full

coverage. Management is kept informed with detailed reports that serve as the basis for quarterly and annual certification reviews.

Change Notification Policy

Symantec ESM provides for a daily audit using the policy that monitors and reports on changes to infrastructure (involved in financial reporting) that may impact system security. All changes made are reported whether authorized or not. Detailed, timely reports keep management informed and enable them to meet disclosure requirements.

Resource Review Policy

Symantec ESM provides for a weekly report on the authorization and privilege configuration of resources (user accounts, files, processes, etc.) used to manage and report financial data. This policy assures these configurations are consistent with enterprise needs and business practices. These checks can be used to assure the enterprise continues to meet SOA requirements for administrative and technical controls.

Symantec's Enterprise Security Manager provides enterprises with the tools necessary to define, measure and report on the compliance of their information systems to industry, regulatory and corporate security policies and standards. ESM supports enterprises in their compliance efforts by:

1. Defining system configuration standards
2. Providing the evaluation checks needed to evaluate and identify potential security problems,
3. Supporting a range of operating system platform (Windows, Unix, Linux, NetWare, OS/400, VMS) settings and configurations
4. Supporting a range of databases and applications (Oracle, MS SQL Server, DB2, Check Point Firewalls, Web Servers) settings and configurations
5. Maintaining lists of files, patches, registry keys and other objects to be checked
6. Providing a snapshot comparing the real world to baseline settings

Symantec ESM supports a wide range of regulatory and standards-based polices including FISMA (NIST 800-53), VISA CISP, NERC, SANS Top 20 List, CIS Benchmarks, HIPAA, ISO/IEC 17799 and so on. Symantec provides policies that cover both hosted and distributed systems running operating systems and applications.

The Final Word

Current industry and operating trends are toward operational environments that ease user access while supporting applications with more complex, dynamic interactions, interdependencies and less control over potential users. Openness, complexity, dynamic and interacting are words that excite the pulse of creative applications developers and challenge the imagination of business managers. Unfortunately, these same words raise the blood pressure of executives and IT managers responsible accountable for the integrity, security and maintenance of all enterprise data but especially confidential and financial information.

Today's enterprise consists of a mix of host-based and distributed infrastructure. Each type of system comes with very different capabilities for auditing. Host-based solution architectures are designed with privileged auditing login functions that allow more accurate data collection and powerful auditing tools. Distributed environments with their proliferation of laptops, PCs, network devices and other special

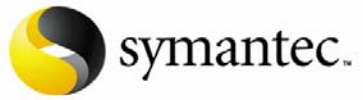
purpose devices do not typically have privileged audit capabilities available. In such cases, non-privileged auditing will have to suffice. Non-privileged audits can still be the source of important and necessary audit report information. Hence, a combination of host and network monitoring capabilities will provide the most complete and effective solution for policy compliance. Balancing easy, open access with security in today's heterogeneous operating environment, especially in the face of increasingly sophisticated and subtle attacks, requires a well thought through strategy combined with exceptional tools. Symantec ESM provides just such a tool.

Monitoring compliance with mandated regulations and policy enforcement have become an unfortunate fact-of-life for enterprises operating in an increasingly litigious and competitive society. We examined Symantec Enterprise Security Manager with Sarbanes-Oxley compliance policies and found it to provide a unique and exceptional range and functional flexibility that addresses the problems of managing compliance for both host-based and distributed architectures. The family of solutions which make up Symantec ESM for compliance management effectively and efficiently meets the needs of enterprises committed to implementing a flexible compliance management strategy.

APPENDIX 1 – Relevant Legislation and Standards

	Name	Industry	Description
Regulations	SOA	Publicly Traded US Corporations	"Sarbanes-Oxley Act of 2001" or "The Public Company Accounting Reform and Investor Protection Act" www.sarbanes-oxley.com
	GLBA	Financial Services Law	"Gramm-Leach-Bliley Act of 1999", or "Financial Services Industry Modernization Act of 1999" www.ftc.gov/privacy/glbact
	FISMA	Federal Agencies	"Federal Information Security Management Act of 2002" http://csrc.nist.gov/sec-cert/
	HIPAA	Health Care	"Health Insurance Portability And Accountability Act of 1996" www.cms.hhs.gov/hipaa
	NERC	Utilities (Power)	"North American Electric Reliability Council" www.nerc.com
	Basel II Accord	International - Banking	"Basel Committee on Banking Supervision new accord" (EMEA) http://www.bis.org/bcbs/index.htm
	PIPEDA	Canadian Privacy	"Personal Information Protection and Electronic Documents Act" http://www.privcom.gc.ca/legislation/02_06_01_e.asp
Standards	ISO/IEC 17799	International - Baseline	"International Standards Organization Standard 17799" www.iso-17799.com
	SANS Top 20	General Security	"Systems Administration and Network Security Institute Top 20 List" www.sans.org
	VISA CISP	Banking	"VISA International Cardholder Information Security Program" http://usa.visa.com
	CIS Benchmarks	World Wide Consortium	"Center for Internet Security" www.cisecurity.org
	COSO	Volunteer Private Sector	"The Committee of Sponsoring Organizations of the Treadway Commission" (COSO) www.coso.org
	COBIT	ISACA	"Control Objectives for Information and related Technology (COBIT)" www.isaca.org/cobit.htm

This white paper was sponsored by: Symantec Corporation



About Ptak, Noel & Associates

With a belief that business success and IT success are inseparable, Ptak, Noel & Associates works with clients to identify, understand and respond to the implications of today's trends and innovations on the future of IT Operations.

www.ptaknoelassociates.com

About the Author

Richard Ptak has over 30 years experience in systems product management working closely with Fortune 50 companies in developing product direction and strategies at a global level. Previously Ptak held positions as senior vice president at Hurwitz Group and D.H. Brown Associates. Earlier in his career he held engineering and marketing management positions with Western Electric's Electronic Switch Manufacturing Division and Digital Equipment Corporation. He is frequently quoted in major business and trade press such as Investor's Business Daily, The New York Times, The Wall Street Journal, BusinessWeek, ComputerWorld, eWeek, and InformationWeek. He is author of "Manager's Guide to Distributed Environments," (John Wiley & Sons, 1998). In addition, Ptak was technical editor of "Cisco Internet Architecture Essentials Study Guide: Cisco Internet Solutions Specialist" by Mathew Recore, Jeremy Laurenson, and Scott Herrmann (Cisco Press, 2002). Ptak holds a master's in business administration from the University of Chicago and a master of science in engineering from Kansas State University.

rlptak@paknoelassociates.com