



Managing Regulatory Compliance
Why it's essential to understand
and manage your IT compliance risk.
And how Symantec's strategic
approach can help you do it.

A host of new laws and regulations governing the security and protection of corporate information is putting pressure on organizations to find efficient ways to achieve compliance.

What's required is a strategic approach that helps you understand and eliminate the root causes of non-compliance.

With market-leading security and availability solutions backed by the industry's deepest expertise, Symantec can help you meet the requirements of today's major laws, standards, and regulations.

Today's compliance landscape

As the compliance landscape becomes more complex, the risks associated with non-compliance grow more costly. Beyond exposure to legal liability and financial penalties, the threats to a company's reputation and the confidence of customers, partners, and corporate stakeholders are significant. While the compliance challenge is large—especially for already overstretched IT staffs—there is good news: Despite the broad focus of many federal, state, and international laws and regulations, considerable progress can be achieved by simply following established best practices for ensuring the security and availability of information assets within your IT infrastructure and documenting the process to demonstrate compliance.

From Sarbanes-Oxley to the Patriot Act, it's a daunting environment

Regulatory bodies and government agencies worldwide are demanding that organizations meet unprecedented standards for data availability, integrity, and security. But secure data retention is only part of the equation. Companies must also be able to retrieve and produce data in a timely manner upon request, as well as demonstrate the existence of IT controls for data retention. Meeting these conditions has become a core requirement. And the way your organization addresses them can have a major impact on operations: As the regulations expand, oversight boards and consumers are looking more closely at the security and availability policies a company uses to ensure privacy and data protection. Relationships with partners are also coming under closer scrutiny as responsibility for compliance is passed down the supply chain to contractors and their subcontractors. (See page 14 for an overview of the IT compliance requirements of the major laws, regulations, and standards affecting organizations today.)

While corporations today are investing significant amounts of time and resources to adhere with the many standards, laws, and regulations that exist, a key challenge in the years to come is developing cost-effective, automated and repeatable IT controls to sustain compliance.

At the same time, the IT infrastructure faces new challenges and cyberthreats that are exposing it to new vulnerabilities. For one, data must now be managed throughout its lifecycle to ensure that it is not altered, inappropriately accessed, or destroyed before its retention period expires. Plus, the skill level required to launch attacks continues to decline while more and more companies are opening their networks to partners and customers, blurring the distinction between trusted visitors and unwelcome intruders. This convergence of trends is driving demand for solutions that address compliance by protecting critical information assets while simultaneously making those assets available to the parties that need them.

The key dimensions to compliance

Information security and availability are two key dimensions along which compliance is measured.

To help your organization get there, follow this three-step approach:

1. Assess your current compliance posture
2. Establish IT controls
3. Sustain IT controls compliance

1. Assess your current compliance posture



Many companies are taking a strategic approach to satisfying the mandates of regulatory bodies. Understanding that most solutions essentially require the same protocols, they are building a framework of security and availability policies that, as an important side benefit, offer substantial positive impacts on cost containment and process standardization.

Your organization first needs to understand its current posture by conducting an assessment of enterprise compliance risk. This will determine where you are and where you want to be, and help define the scope of the effort you are undertaking—how big the job is and what resources are required. A gap analysis will provide a clear view of where your IT team needs to focus its attention. Then you can establish a checklist of the people, processes, and technologies that will be required to achieve compliance.

Assess risk across the enterprise

First, you need to conduct an audit of your company's IT infrastructure to identify security, network, and data and application availability risks. Start by creating a baseline inventory of all in-scope assets, systems, security and availability controls. What hardware and software is currently installed and who has access to programs and data? Are there existing controls for change management, intrusion detection and prevention, patch management, application and data availability, backup and recovery, and records retention and archiving? Are these controls centralized at the data center or do they extend to individual users and remote offices? How are critical systems configured and what is the state of controls on those systems?

Symantec can help you analyze the effectiveness of IT processes and controls for maintaining the security and availability of critical information resources. A complete analysis will enable your team to identify IT control deficiencies, such as inappropriate access levels or improper segregation of duties. And it will help you close any gaps between the current state and the desired one.

Evaluate against industry best practices

Once you create a baseline of your existing security and availability controls and identify and prioritize gaps, you will want to evaluate your preparedness for achieving a state of compliance with IT controls. You might ask, which regulations apply to your business or what does being “compliant” really mean? You need to have a solid understanding of what auditors are looking for and how each law and regulation impacts your business.

A good place to start is with well-established industry standards. A gap analysis with ISO 17799 will provide an assessment of your security program against industry best practices and can offer guidance for improving your overall regulatory program. In addition to auditing security controls, current data retention and protection processes must be evaluated to ensure that they not only meet compliance requirements, but are also adequate in the event of a legal inquiry calling for the discovery and production of electronic correspondence.

Today's enterprise faces a growing number of risk factors. According to Symantec research, external threats to data confidentiality increased by 148% in 2003. Likewise, the number of internal software vulnerabilities that might allow those threats to penetrate networks has risen steadily over the past five years. Put the two trends together and the potential risks to data are considerable.

1. Assess your current compliance posture (cont.)

The Symantec Approach

- Assess risk across the enterprise
- Evaluate against industry best practices
- Identify security and availability vulnerabilities

Symantec offers a family of powerful products and services to help organizations analyze the current posture of their compliance program:

- Symantec Standards Compliance Assessment Service
- Symantec Network Vulnerability Assessment
- Symantec Risk Assessment Service
- Symantec Systems Continuity Service
- Symantec DeepSight™ Alert Services
- Symantec Enterprise Security Manager™
- Symantec Discovery™
- VERITAS Business Continuity Management Service

Identify security and availability vulnerabilities

Your team should assess technical vulnerabilities to identify missing or inadequate controls that might increase exposure to data loss or downtime. Symantec offers solutions that provide real-time vulnerability intelligence and a prioritized view of exposures, enabling you to accurately assess technical risks and set priorities for closing gaps. An assessment will uncover systems and data exposed in the event of a business disruption, as well as information that is not sufficiently protected, cannot be easily retrieved, or has been archived beyond the required period.

At this stage, you also need to classify assets based on business value and criticality. By assigning business value to data, the appropriate protection and retention policies can be created. You should also prepare policy recommendations to help your business protect against and rapidly recover from system attacks, faults, or site outages, which will help meet regulatory compliance requirements and maintain continuous availability of systems and data.

Ask the right questions

Would a disruption impact your ability to access critical applications and data? In the event of a legal inquiry, what is your process for discovery of requested email? What happens to data when it is no longer required? Asking these kinds of questions will help you understand the risks and identify what additional controls should exist.

2. Establish IT controls

After assessing your compliance posture, it's time to address vulnerabilities and manage any control gaps that have been discovered. By establishing systematic controls to mitigate risks, you improve your organization's ability to demonstrate regulatory compliance.

Design and implement controls

First you need to design controls that support your security and availability requirements—at headquarters and branch offices, and for remote workers and partners. Your team should look at strategies for managing change within your infrastructure and focus on areas such as asset, incident, and patch management. Controlling access to programs and data is an important element of a control environment. You need to ensure critical data and applications are protected from malicious code, network penetration, unauthorized access, and other violations. IT controls should be implemented to minimize the risk of data loss and downtime, sustain access to business-critical systems and applications at all times, and recover systems in the event of a device failure or site outage.

Standardized policies should also be set for record retention, protection, and retrieval based on their business value and compliance requirements. Implementing a secure means of retaining data throughout its lifecycle, as well as a timely and efficient way of discovering and retrieving records for compliance or legal inquiries is essential.

Establishing controls for records is critical

According to Osterman Research, 54% of organizations have no policies or systems in place to prevent users from deleting messaging system content that is important to retain on a long-term basis.¹

The Symantec Approach

- Design and implement Controls

Symantec offers a comprehensive family of products and services to help organizations automate the management of IT controls:

- Symantec Discovery
- Symantec Consulting Services
- Symantec™ Managed Security Services
- Symantec DeepSight Alert Services
- Symantec Enterprise Security Manager
- Symantec™ Incident Manager
- Symantec LiveState™ Client Management Suite
- Symantec™ Gateway Security
- Symantec™ Network Security
- Symantec™ Client Security
- Symantec LiveState™ Recovery
- VERITAS NetBackup
- VERITAS Cluster Server
- VERITAS Volume Replicator
- VERITAS Storage Foundation
- VERITAS Enterprise Vault

¹ *Messaging Security Market Trends 2005-2008*. Osterman Research, May 2005.

3. Sustain IT controls compliance



The sheer amount of data that needs to be retained has increased exponentially and, when coupled with more stringent retention requirements, has created explosive growth in storage costs and an increased risk of implementing an inadequate data retention strategy. According to a recent survey conducted by Osterman Research, 65% of organizations consider growth in messaging storage to be a serious or very serious problem, second only to the problem of spam.²

² *Messaging Security Market Trends 2005-2008*. Osterman Research, May 2005.

To meet the demands of regulators and all internal and external constituencies, your team must rigorously measure the state of IT controls; remediate gaps and variances, and document; record, and report on the adequacy of IT controls. A variety of information management solutions can help you create a best practices environment for audit, oversight, and governance—and contribute to your success.

Measure and test control status

Real-time monitoring is necessary to measure the effectiveness of the controls you have implemented and report possible breaches. At a minimum, you should conduct periodic technical assessments of IT controls and policies. For instance, are firewalls configured properly, are operating systems hardened with the appropriate levels of user access, and are your backup and recovery procedures meeting service level agreements?

To reduce the probability of compromise and satisfy regulatory requirements, security and availability controls must be continuously measured. In order to ensure timely and accurate testing of controls, it is important to automate the detection of deviations from the desired state and provide an audit trail of policy compliance. For instance, to monitor availability controls the status of all backup and recovery activities should be logged and reported on and disaster recovery scenarios tested and validated on a periodic basis.

Remediate control gaps

In any environment, control gaps will undoubtedly be discovered, which means you must identify potential fixes to improve policies and ensure that IT controls are compliant. Consider standardized solutions that proactively detect and prioritize incidents, discover changes against the desired security baseline, and automatically correct the problem—be it installing patches, removing unauthorized software, or updating attack signatures. To sustain access to critical data and applications, end-to-end availability solutions should proactively monitor the infrastructure and support policies for automatically detecting an error or security breach and taking action, such as failing over an application to a healthy server or recovering data in its original state in the event of a fault. By automating the process of documenting, testing, auditing, and remediating IT controls, you are able to reduce costs and gain efficiencies while sustaining controls compliance.

Adapt to change with agility

Outsourcing security services can provide protection and valuable feedback to help overstretched security teams. For instance, early warning and threat management services provide real-time intelligence on emerging threats and evolving vulnerabilities. Armed with actionable information the services provide helps ensure an optimal response and enables your team to adapt to change with agility by adjusting the mix of people, processes, and technologies your compliance program requires.

Of the 700 publicly traded companies recently surveyed by the accounting firm PricewaterhouseCoopers, only about 20% are on schedule to meet the data control requirements for 2005 mandated by the Sarbanes-Oxley Act.³

³ As Sarbanes-Oxley Looms, Companies Rush to Comply. *InformationWeek*, 16 November 2004.

Some statistics to put it in perspective: Currently, about 60% of IT regulations mandate data privacy and identity theft protection procedures, 30% mandate a well-defined and well-managed information security program, and 10% deal with issues such as sharing information with the government.⁴

⁴ *Tackling Security Compliance Challenges*. Forrester Research, Inc., February 2004

3. Sustain IT controls compliance (cont.)



Symantec's global intelligence network can help your team stay on top of the latest threats in a rapidly evolving security environment. Symantec tracks vulnerabilities in more than 18,000 product versions from 2,200 vendors, and delivers detailed intelligence advisories on real-time security incidents gathered from more than 20,000 sensors in 180 countries worldwide.

Report on compliance

An information security and availability solution that promotes compliance will have the ability to integrate, interpret, and present information regarding the state of IT controls. To effectively monitor your compliance posture, your team should implement a holistic capability that detects unauthorized access, potential compromises to data integrity and availability, and other security breaches across all platforms and technologies. It should have robust analysis and reporting capabilities such as the ability to capture and produce upon request all archiving, search, discovery, and retrieval activity.

Provide validated status

An effective solution must be able to define security and availability policies and demonstrate that processes are being followed and are auditable. It must also aggregate, correlate, and analyze data to produce information in a format that is useful to oversight and governance bodies. Via customized reports that document and assess previous and current states of compliance, your team can discover trends and gaps that will be useful in developing remediation strategies.

Establish a culture of compliance

Finally, you should conduct a security awareness audit, the results of which can be used as a benchmark to measure the progress of employees in understanding security policies and complying with them. Based on the results of the audit, you can implement a training and communications program that includes tools such as computer-based tutorials and other resources to help your organization meet regulatory requirements for employee security awareness training.

The big picture

Compliance is a broad, complex issue with far-reaching implications. But when you look at the big picture, most laws and regulations are basically asking you to pay attention to four key areas: accountability, risk analysis, IT controls, and governance. To succeed the executive team must understand that it is ultimately accountable and must take proactive measures to manage compliance. In the end, establishing a culture of compliance in your organization all comes down to good governance and oversight.

The Symantec Approach

- Measure and test control status
- Remediate control gaps
- Adapt to change with agility
- Report on compliance
- Provide validated status
- Establish a culture of compliance

Symantec offers a family of powerful products and services to help organizations maintain oversight and governance as part of an IT compliance program:

- Symantec Security Awareness Training Program
- Symantec Enterprise Security Manager
- Symantec™ Security Management System
- VERITAS NetBackup
- VERITAS Enterprise Vault
- VERITAS Cluster Server
- VERITAS Volume Replicator
- VERITAS Storage Foundation
- VERITAS CommandCentral Service

Compliance delivers an expanded set of benefits

Three easy steps to sustaining IT compliance? Not quite. It's hard work that requires the right set of people, processes, and technologies, along with insightful risk mitigation, systematic controls, agile remediation, and constant oversight. But, it's well worth the effort. By taking a proactive approach to understanding the risks and ensuring the security and availability of your information assets and systems, you build a foundation that makes it easier to achieve and sustain compliance.

And by establishing automated and standardized controls to prevent intrusions and disruptions, reducing the risk of data loss and downtime, implementing secure record retention and discovery capabilities, and leveraging actionable intelligence, the program you develop will be easier to sustain over time. Which brings major benefits to your IT organization and your company as a whole:

- Protect sensitive information while making it recoverable and retrievable in its original state and in a timely manner
- Enhance operational efficiencies through the automation of processes, resulting in cost minimization and revenue protection
- Maximize system uptime and service availability, and minimize the impact of business disruptions
- Create a flexible IT architecture that can easily adapt to future changes in laws, regulations, and overall business needs
- Improve consistency by standardizing business processes and the reporting of IT internal controls, thereby realizing economies of scale to reduce the complexity and associated risks of inconsistent controls
- Add value to the overall business in terms of brand reputation, customer satisfaction, and investor confidence by improving the integrity of the company's assets and systems

To ensure regulatory compliance requires a resilient IT infrastructure that enables critical assets to be both secure and available. Symantec can help you get there via an approach we call Information Integrity.™ It's a balanced approach that makes information available wherever, whenever, and to whomever your business needs dictate.

Keep your business up, running, and growing no matter what happens

Symantec's comprehensive product and service portfolio offers the industry's broadest range of solutions for ensuring Information Integrity. Our offerings provide the visibility and expertise you need to determine what's important and how best to act on it. And Symantec can help you establish processes to increase the efficiencies of your IT security and operations teams and align them towards the same goal: To build an IT infrastructure that ensures the security and availability of information to sustain IT compliance.

Key laws and regulations

A variety of federal, state, and international standards, laws, and regulations affect many businesses and public agencies worldwide and impose standards for how these entities address the issue of provisioning information security and availability. Here are some of the most significant mandates:

Sarbanes-Oxley Act (SOX) of 2002. For publicly traded companies and accounting firms, SOX is the most important piece of legislation affecting corporate governance and accountability in years. The law mandates controls and standards for financial disclosure, as well as ensuring the confidentiality, integrity, and availability of financial reporting information. Personal certification by the CEO and CFO add pressure and give top management a tangible interest in compliance.

Gramm-Leach-Bliley Act of 1999 (GLBA). Also known as the Financial Services Modernization Act, GLBA applies to banks, securities firms, insurance companies, and other financial institutions. The act mandates the privacy of customer records and requires safeguards to protect them.

New Basel Capital Accord (Basel II). Published by the Bank for International Settlements, Basel II proposes new standards for measuring risk within banks conducting international monetary transfers. In addition to credit and market risk, for the first time, operational risk must also be calculated to determine minimum capital reserve levels.

EU Data Protection Directive. This legislation is aimed at protecting personal information of EU residents. It restricts the transfer of personal information between EU and non-EU countries. The Directive applies to the processing of data, including restrictions on obtaining, using, disclosing, erasing, recording, and retaining personal information. The Directive is followed by several member states, many of which have also passed their own laws harmonizing with the Directive, such as the UK Data Protection Act of 1998.

New regulations and auditing requirements are driving a growing number of Global 2000 companies to create dedicated information security groups that are separate from IT operations. The META Group projects that 80% of the companies that will be affected by the Sarbanes-Oxley Act in 2005 will create new security programs to address corporate governance issues raised by the law.

Health Insurance Portability and Accountability Act (HIPAA). In addition to ensuring health insurance portability, HIPAA stipulates a number of requirements with respect to the security and privacy of patient information.

Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11). 21 CFR Part 11 affects all FDA-regulated industries, including biopharmaceuticals, personal care products, and food and beverages. The legislation mandates that companies adhere to strict technical procedures regarding the use and archiving of electronic records.

Securities and Exchange Commission (SEC) Rules 17a-3 and 17a-4. The SEC outlines the types of communications that must be retained by certain exchange members, brokers, and dealers for a minimum of six years, the first two of which must be in an easily accessible place.

National Association of Securities Dealers (NASD) Rules 3010 and 3110. Firms subject SEC Rules 17a-3 and 17a-4 must establish a system for the supervision of the activities of their members, brokers, and dealers, including their correspondence with the public. This requires a process for periodic search and review of all electronic communications. In addition, member firms must implement a record retention strategy for all customer records and transaction data in an auditable format that must be stored in an easily accessible place.

Federal Information Security Management Act (FISMA). This new act requires each federal agency to implement and document a program to provide security for its information systems and assets.

ISO 17799. Developed by the International Standards Organization, ISO 17799 represents best practices in information security controls and policy management.

Information Security Forum (ISF). The Standard of Good Practice for Information Security is a business-focused statement of best practices published by ISF members, including some of the world's leading IT research and risk management organizations.

Technology alone cannot achieve regulatory compliance. You also need a partner you can trust. Working with Symantec, your team can leverage the tools and expertise of an industry leader to implement proactive, effective solutions.

Symantec's proven security, systems, and storage solutions and our unrivaled enterprise experience can help you understand and manage compliance risk. For details visit www.information-integrity.com.

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.

Symantec has worldwide operations in more than 40 countries. 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

Symantec, the Symantec logo, and VERITAS are U.S. registered trademarks of Symantec Corporation. Information Integrity is a trademark of Symantec Corporation. All other brand and product names are trademarks of their respective holder(s). Copyright © 2005 Symantec Corporation. All rights reserved.
07/05 10363082