

# Symantec™ Control Compliance Suite

Automating and managing IT compliance as an ongoing process to reduce cost and complexity

---

## Overview

Symantec Control Compliance Suite (CCS) automates key IT compliance processes. Symantec Control Compliance Suite helps organizations ensure coverage of external mandates through written policy creation, dissemination, acceptance tracking, and exception management. Furthermore, CCS can actually demonstrate compliance to external and internal policies by automating the assessment of technical and procedural controls and evaluating the assessment against risk criteria. Evidence of compliance can be agentlessly gathered on configurations, permissions, patches, vulnerabilities, and manual attestation of procedural activities. Symantec Control Compliance Suite also helps organizations fix deviations to standards, enabling immediate corrective actions or triggers to third-party response workflow systems.

---

## The need to automate key IT compliance processes

Today, the complexity of ensuring compliance and strong IT governance in an organization is made more difficult by the variety of security issues that must be monitored and the need to comply with multiple external mandates.

Recent research indicates that companies investing in one-off solutions for each compliance mandate they face will spend significantly more on IT compliance than those that develop a single solution to manage multiple mandates.

The action most responsible for best-in-class compliance results is the frequent measurement of IT-based controls, policies, and audit results. Industry leaders are monitoring,

*\*Improving IT Compliance: 2006 IT Compliance Benchmark Report," June 2006*

measuring, and reporting on these once every 21 days and are conducting internal audit and IT security monitoring eight times more frequently than are industry laggards.\*

Unfortunately, the majority of costs associated with implementing strong IT compliance come from often-repeated, time-consuming processes: creating/defining/distributing policies, tracking exceptions, managing standards, managing entitlements, remediating deviations, and performing both procedural and technical assessments. Thus, the critical need for organizations is finding a way to perform these costly processes in a more efficient manner.

Furthermore, organizations are struggling not just with maintaining strong IT compliance, but also with understanding what policies and standards they should be implementing to achieve it. A typical organization is a complex, heterogeneous environment, with a variety of platforms and a diverse set of control objectives.

Understanding what is required and how to achieve strong IT compliance requires comprehensive intelligence of regulations, frameworks, and the relevant best practices.

---

## Symantec Control Compliance Suite

The Symantec Control Compliance Suite is an integrated set of technologies that enable the key processes needed to achieve and maintain IT compliance. By providing these technologies in a single solution, CCS can make the process of compliance easier and more cost-effective for customers.



### Policy module

The Policy module assists with defining and mapping policies to best practices, frameworks, and regulations, and identifies overlaps in control objectives to reduce duplicative assessment efforts. The Policy module also automates the distribution of written policies throughout the organization, tracking end-user policy acceptances and exception requests. The Policy module collects evidence of compliance to control objectives through integration with other Symantec Control Compliance Suite components that provide both procedural and technical assessments, thus enabling analysis and reporting on compliance efforts. In addition, the Policy Module ships with sample policies and policy templates to jump-start a strong governance process.

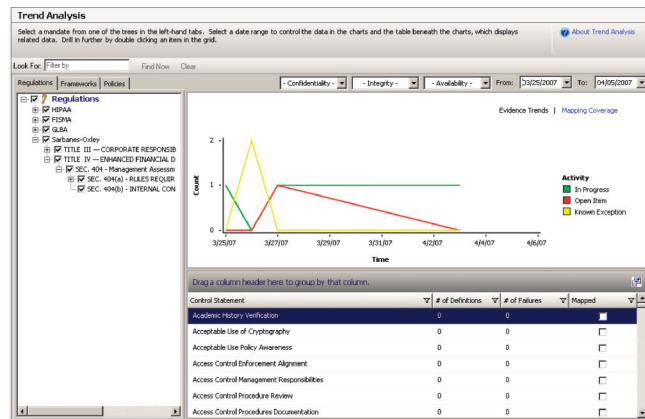


Figure 1. Policy Module—trend analysis

### Entitlement module

The Entitlement module gathers effective permissions on data from across the enterprise, translates those permissions into a consistent human-readable format, associates management classification to the data, and electronically routes the information to business owners for access approval. Entitlements approvals are tracked and tied to analysis/audit reports as controls evidence.

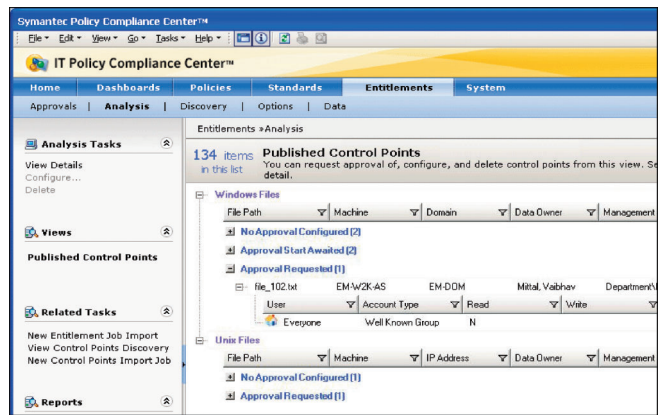


Figure 2. Discovery and configuration of entitlement control points

### Response Assessment module

The Response Assessment module automates the assessment of non-programmatic controls. These non-programmatic controls make up the majority of objectives laid out in regulations/frameworks. Organizations often rely on paper-based assessments that are expensive and difficult to manage. RAM manages the manual assessment process from questionnaire creation and distribution to analysis of response data. RAM integrates with Symantec Control Compliance Suite to provide a comprehensive view of both procedural and technical controls, thus ensuring policy coverage.

### Standards module

The Standards module automates the management of deviations from technical standards and makes it possible to remediate misconfigurations. The Standards Module provides prepackaged technical standards that granularly define best practices for securing servers and databases and trends compliance to these standards. In addition, the CCS Standards Module provides detailed remediation instructions to correct deviations and integrates with existing change control ticketing systems to ensure that changes are made only after appropriate authorization and with proper oversight.

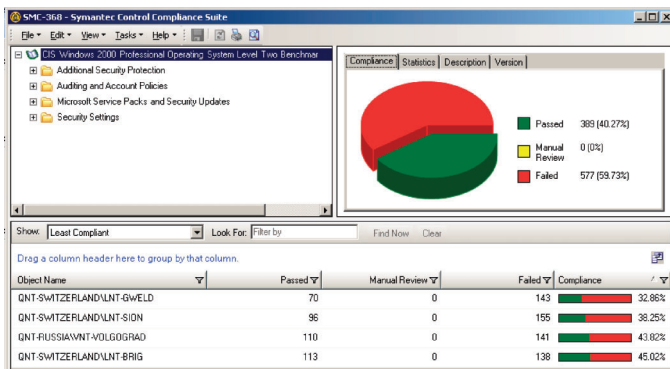


Figure 3. Technical controls assessment and reporting

## Technical specifications

### Supported platforms for the Standards Module

<b>Windows</b>	Windows® XP, x64, Windows Vista™, Windows Server® 2000/2003/R2, Windows NT® 4.0, Active Directory®
<b>Exchange</b>	Mobile Devices, 5.5, 2003, 2000
<b>NetWare®</b>	6.5, 6, 5, 4, NDS eDirectory
<b>Red Hat</b>	EL 4.0, 3.0, 2.1, v9, v8
<b>SUSE</b>	ES 9.0, ES 8.1, v9.3, v9.2, v9.1, v9.0, v8.2, v8.1, v8
<b>Solaris™</b>	10, 9, 8
<b>HP-UX</b>	11.23, (11i v2), 11.11, (11i v1), 11
<b>AIX®</b>	5.3, 5.2, 5.1
<b>Databases</b>	Oracle® 10g, 9i, 8i, Microsoft® SQL Server 2005, 2000, 7.0, Microsoft SQL Server 2005 Auditing

## System requirements

### Server/Web portal/database minimum hardware requirements

- 3.0 GHz CPU
- 1 GB RAM
- 1 GB free disk space
- Monitor resolution set to 1024x768 pixels or greater
- Microsoft Windows 2000, Windows Server 2003, Windows XP, or later
- Microsoft .NET Framework 2.0

### Client minimum hardware requirements

- 1.2 GHz CPU
- 512 MB RAM
- Monitor set to 1024x768 pixels or greater
- Microsoft Windows 2000, Windows Server 2003, Windows XP, or later

## Endorsements

- Information Security Magazine, 2007 Readers' Choice Award
- Best Policy Monitor: 2004 Network Computing Well-Connect Awards
- Best Policy Management Solution: 2004 SC Magazine Global Awards
- 2003 Network Computing Editor's Choice Award
- IDC white paper: "Optimizing Your IT Controls Environment for Compliance with Multiple Regulations," by Charles Kolodgy, December 2005

**Key Features and Benefits**

Features	Benefits
Policy module	<p><b>Define and manage written policies</b></p> <ul style="list-style-type: none"> <li>Includes regulation and mandate content for Sarbanes-Oxley, PCI DSS, FISMA, HIPAA, GLBA, Basel II, and NERC</li> <li>Includes framework content for ISO 17799, COBIT (v3 and v4), and NIST SP800-53</li> <li>Sample policies and policy templates provide a starting point for strong IT compliance</li> </ul> <p><b>Distribute policies and track acceptance</b></p> <ul style="list-style-type: none"> <li>Target dissemination of policies to specific end-user groups</li> <li>Log all acceptance information for reporting and audit purposes</li> <li>Ensure that exceptions are reviewed/approved by appropriate policy owners and tagged with an expiration date</li> </ul> <p><b>Map policies to regulations or frameworks to ensure and demonstrate coverage</b></p> <ul style="list-style-type: none"> <li>Report on compliance posture to multiple mandates</li> <li>Uniquely demonstrate compliance to policy by collecting evidence from procedural and technical data sources</li> </ul> <p><b>Collect and display evidence for control objectives</b></p> <ul style="list-style-type: none"> <li>Provide best practice guidelines that translate vague regulatory requirements to actionable policy and collected evidence</li> <li>Perform risk-based analysis via an Impact Index (incorporating Confidentiality, Integrity, and Availability attributes to collected evidence)</li> <li>Map evidence directly to control statements, improving traceability between evidence and frameworks/regulations</li> </ul>
Entitlement module	<p><b>Gather effective permission</b></p> <ul style="list-style-type: none"> <li>Multiplatform support for Windows®, UNIX, Linux®, and Novell®</li> <li>Automated discovery of control points based on files/directories/groups</li> </ul> <p><b>Report on effective permissions</b></p> <ul style="list-style-type: none"> <li>Translate permissions into consistent human-readable format</li> <li>Search through and find data privileges easily</li> </ul> <p><b>Provide workflow for effective entitlements management</b></p> <ul style="list-style-type: none"> <li>Assign business owners to operational data</li> <li>Route entitlements to data owners for review and approval</li> <li>Ensure periodic review and approval of entitlements</li> <li>Define management classifications</li> <li>Enable business owners to effectively engage with IT when changes are needed</li> </ul>

Features	Benefits
Response Assessment module	<p><b>Questionnaire creation and distribution</b></p> <ul style="list-style-type: none"> <li>Assess, store, and report responses for procedural controls data</li> <li>Provides out-of-the-box content based on popular standards and frameworks: BS 7799, COBIT, COSO, CSC, C-TPAP, HIPAA, FAA, FERPA, FFIEC, FISMA, GLBA, ISO 14001, ISO 27001, ISO 27799, ISO 20858, ITIL, MDA, OHSAS 18001, ONR 17700, PCI, NERC, NIST, and SOX</li> <li>Provides the ability to quickly create custom questionnaires</li> <li>Allows for multi-path (branching) assessment questions</li> <li>Supports many response types, including radio button, freeform, check boxes</li> <li>Deploys and scales easily using Web-based services</li> </ul> <p><b>Consolidated reporting of response</b></p> <ul style="list-style-type: none"> <li>Saves incomplete questionnaires and permits out-of-order response entry</li> <li>Allows for risk-based weighting of both questions and responses</li> <li>Provides end-user quizzing and certification</li> </ul>
Standards module	<p><b>Create or select technical standards</b></p> <ul style="list-style-type: none"> <li>Broad, heterogeneous platform support allows for enterprise-wide coverage (see table in Technical Specifications)</li> <li>Supplies regulatory content for Sarbanes-Oxley, FISMA, HIPAA, GLBA, and Basel II, and framework content for ISO 17799, COBIT, and NIST SP800-53</li> <li>Includes best practices checks based on CIS, NSA benchmarks, and data from Symantec security experts</li> </ul> <p><b>Assess controls</b></p> <ul style="list-style-type: none"> <li>Agentless technology eases deployment and maintenance</li> <li>Schedules jobs to reduce the cost of redundant and often-repeated technical assessments</li> <li>Integrated internet scanner provides a vulnerability assessment view</li> <li>Dashboard tool creates customizable reporting views of compliance posture</li> </ul> <p><b>Detect deviations</b></p> <ul style="list-style-type: none"> <li>Reports pass/fail scores against standards to provide a view of security and compliance</li> <li>Manages exceptions to technical checks, thus ensuring appropriate review/approval, and automatically accounting for exceptions in reports</li> </ul> <p><b>Remediate deficiencies</b></p> <ul style="list-style-type: none"> <li>Ticketing system integration works within the existing organizational change control process</li> <li>Patch assessment integration with Shavlik HFNetChkPro v5.6 provides centralized interface for patch management</li> </ul>



### More information

*Visit our Web site*

<http://enterprise.symantec.com>

*To speak with a Product Specialist in the U.S.*

Call toll-free 1 (800) 745 6054

*To speak with a Product Specialist outside the U.S.*

For specific country offices and contact numbers, please visit our Web site.

### *About Symantec*

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

### *Symantec World Headquarters*

20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

