

Symantec™ Control Compliance Suite 9.0

Automates key IT activities including risk assessment, policy management, IT controls assessment and monitoring, remediation, and reporting

Overview

Symantec Control Compliance Suite provides end-to-end coverage for the IT compliance lifecycle, including policy management, technical and procedural controls assessment, reporting, and remediation. Control Compliance Suite provides the most comprehensive view of risk and compliance posture with a combination of point-in-time controls assessment and real-time monitoring of risks and threats. Control Compliance Suite is an open architecture that enables integration with business processes and other external solutions.



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, 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.¹

Unfortunately, the majority of costs associated with implementing strong IT compliance come from often-repeated, time-consuming processes: creating, defining, and 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 more efficiently.

Organizations are struggling not just with maintaining strong IT compliance, but also with understanding what policies and standards they should be implementing. 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 cost-effective, strong IT compliance requires comprehensive intelligence of regulations,

1. "Improving IT Compliance: 2006 IT Compliance Benchmark Report," June 2006.

frameworks, and the relevant best practices, and the appropriate tools to automate the process.

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, Symantec Control Compliance Suite can make the process of compliance easier and more cost-effective for customers.

Policy Manager

The Policy Manager assists with defining and mapping policies to best practices, frameworks, and regulations, and it identifies overlaps in control objectives to reduce duplicative assessment efforts. The Policy Manager also automates the distribution of written policies throughout the organization, tracking end-user policy acceptances and exception requests. The Policy Manager 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 Manager ships with over 125 sample policies and policy templates, and it fully and easily customizable. Newly enhanced reporting and dashboard capabilities allow more flexibility for distributing information.

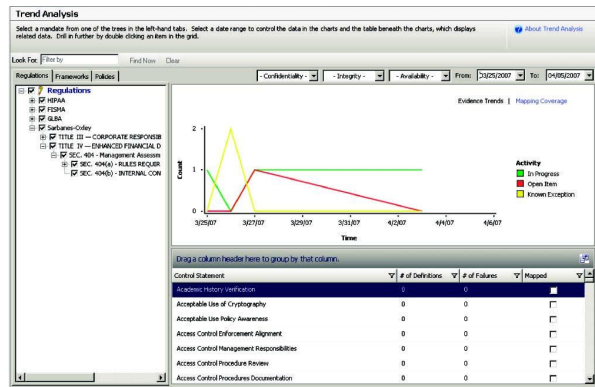


Figure 1. Policy Manager—trend analysis

Entitlement Manager

The Entitlement Manager 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. Entitlement approvals are tracked and tied to analysis/audit reports as controls evidence.

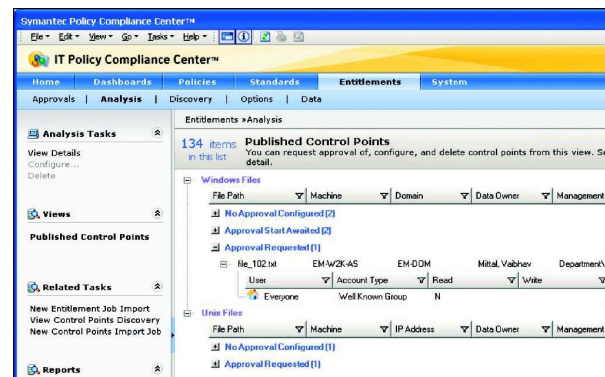


Figure 2. Discovery and configuration of entitlement control points

Response Assessment Manager

The Response Assessment Manager (RAM) 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.

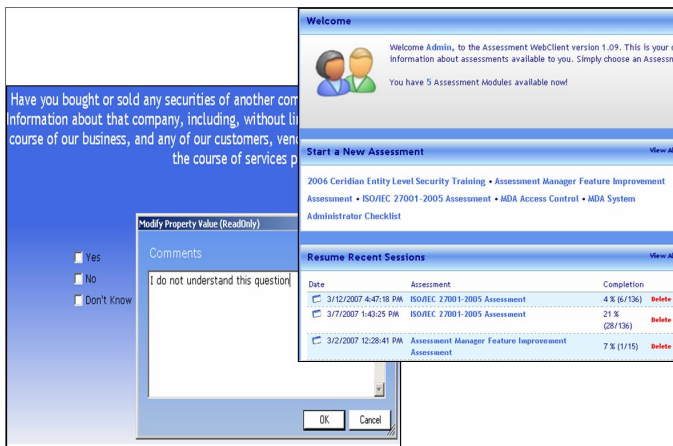


Figure 3. Response Assessment Manager

Standards Manager

The Standards Manager automates the management of deviations from technical standards and makes it possible to remediate misconfigurations. The Standards Manager provides prepackaged technical standards that

granularly define best practices for securing servers and databases and securing trends compliance to these standards. In addition, the Standards Manager of the Symantec Control Compliance Suite 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.

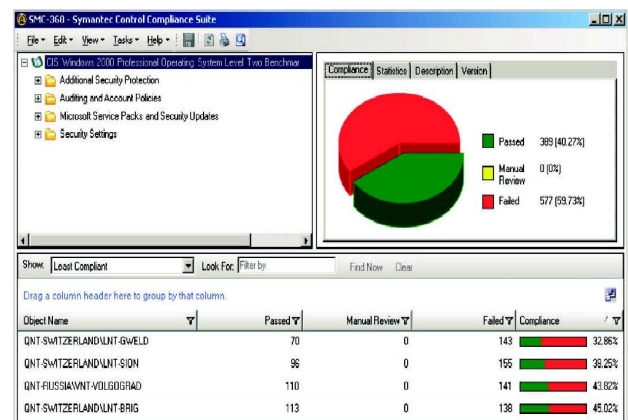


Figure 4. Technical controls assessment and reporting

Security Information Manager

Security Information Manager enables organizations to collect, store, and analyze log data as well as monitor and respond to security events to meet IT risk and compliance requirements. It can collect and normalize a broad scope of event data and correlate the impact of incidents based on their criticality to business operations or the level of compliance to various mandates. Incidents are prioritized using its built-in asset management function—which is populated using

Solution Overview: Compliance and Security Management Symantec™ Control Compliance Suite 9.0

scanning tools, allows confidentiality and integrity, and allows response ratings and policies to be assigned to help prioritize incidents.

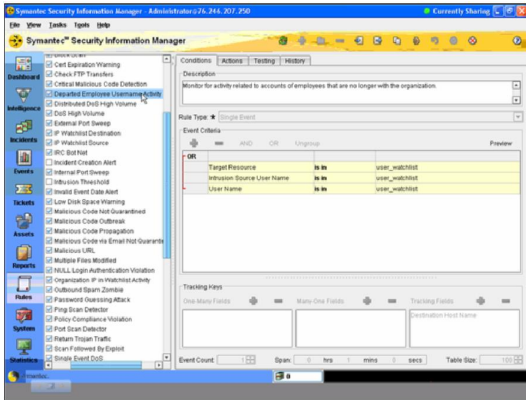


Figure 5. Security Information Manager--user access monitor

Key Features and Benefits

Policy Manager

- Defines and manages written policies
- Includes regulation and mandate content for Sarbanes-Oxley, PCI DSS, FISMA, HIPAA, GLBA, Basel II, and NERC
- Includes framework content for ISO 17799, COBIT (v3 and v4), and NIST SP800-53
- Has sample policies and policy templates that provide a starting point for strong IT compliance
- Includes an easy-to-use policy-creation wizard
- Offers a policy risk rating

- Distributes policies and tracks acceptance
- Targets dissemination of policies to specific end-user groups
- Logs all acceptance information for reporting and audit purposes
- Ensures that exceptions are reviewed and approved by appropriate policy owners and tagged with an expiration date
- Offers enhanced reports and dashboards capabilities
- Maps policies to regulations or frameworks to ensure and demonstrate coverage
- Reports on compliance posture to multiple mandates
- Uniquely demonstrates compliance to policy by collecting evidence from procedural and technical data sources
- Integrates easily through mapping interface
- Enhances integration with exception management and asset systems
- Collects and displays evidence for control objectives
- Provides best practice guidelines that translate vague regulatory requirements to actionable policy and collected evidence
- Performs risk-based analysis via an Impact Index (incorporating Confidentiality, Integrity, and Availability attributes to collected evidence)
- Maps evidence directly to control statements,

Solution Overview: Compliance and Security Management Symantec™ Control Compliance Suite 9.0

improving traceability between evidence and frameworks/regulations

Entitlement Manager

- Gathers effective permissions
- Offers multiplatform support for Windows®, UNIX, Linux®, and Novell®
- Support Oracle® and SQL Server databases
- Automates discovery of control points based on files/directories/groups
- Reports on effective permissions
- Translates permissions into consistent human-readable format
- Has entitlement change reporting capabilities
- Searches and finds data privileges easily
- Provides workflow for effective entitlements management
- Assigns business owners to operational data
- Routes entitlements to data owners for review and approval
- Provides support for second-level approval
- Ensures periodic review and approval of entitlements
- Defines management classifications
- Enables business owners to effectively engage with IT when changes are needed

Response Assessment Manager

- Creates and distributes questionnaires

- Assesses, stores, and reports responses for procedural controls data
- 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
- Provides the ability to quickly create custom questionnaires
- Allows for multi-path (branching) assessment questions
- Supports many response types, including radio button, freeform, and check boxes
- Associates surveys to respondents and assets
- Attaches evidence to survey responses
- Deploys and scales easily using Web-based services
- Integrates with Control Compliance Suite asset system
- Consolidates reporting of responses
- Saves incomplete questionnaires and permits out-of-order response entry
- Allows for risk-based weighting of both questions and responses
- Provides end-user quizzing and certification
- Sets threshold values and retries
- Scores responses

Standards Manager

- Creates or selects technical standards
- Has broad, heterogeneous platform support that allows for enterprise-wide coverage (see table in Technical Specifications)
- Supplies regulatory content for Sarbanes-Oxley, FISMA, HIPAA, GLBA, and Basel II; and framework content for ISO 17799, COBIT, and NIST SP800-53
- Includes best practices checks based on Center for Internet Security Standards (CIS), National Security Agency (NSA) benchmarks, and data from Symantec security experts
- Assesses controls
- Offers agentless technology that eases deployment and maintenance
- Has agent-based technology supporting special platforms (i.e., AS/400, Sybase, MySQL)
- Schedules jobs to reduce the cost of redundant and often-repeated technical assessments
- Provides a vulnerability assessment view via an integrated internet scanner
- Creates customizable reporting views of compliance posture with a dashboard tool
- Detects deviations
- Reports pass/fail scores against standards to provide a view of security and compliance
- Manages exceptions to technical checks, thus ensuring

- appropriate review and approval as well as automatically accounting for exceptions in reports
- Has enhanced check-builder capabilities to allow for better control
- Offers change auditing
- Remediates deficiencies
- Provides ticketing system integration that works within the existing organizational change-control process

Security Information Manager

- Compliance and audit reporting
- Log retention and retrieval
- Real-time threat analysis
- Automated incident prioritization
- Incident remediation workflow
- Aligns security and compliance requirements with IT operations
- Meets compliance reporting requirements quickly and effectively
- Gains accurate and timely visibility into your security risk posture
- Increases IT staff productivity by prioritizing the most critical of security issues
- Reduces IT security operational costs and improve response time
- Provides appropriate security service levels to different business units and geographies

Fully Integrated and Automated

Risk Based

Flexible Deployment

New / Enhancement to Control Compliance Suite 9.0 Infrastructure

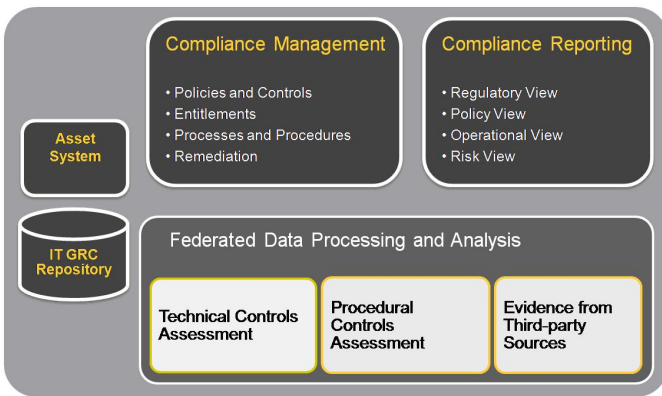


Figure 8. Control Compliance Function overview

Asset System

The Control Compliance Suite Asset System provides scheduled, automated import of asset information from Asset management systems, CMDBs, etc. With the new Asset System and data repository, companies can now take an asset-centric approach to compliance and risk management. Through the Asset System's automated

reconciliation capabilities, customers will have the most up-to-date information about an asset.

- Centralized asset store with multiple predefined types
- Asset Location Site—New concept for associating assets to enterprise location
- Uses CSV data collector for custom asset types
- Automated reconciliation and manual review
- User interface views of compliance measurement, risk scores, evidence, etc.

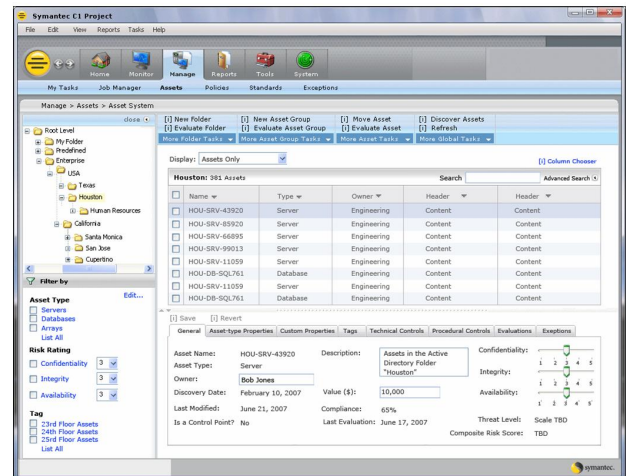


Figure 7. Assess management user interface

Risk scoring

Control Compliance Suite allows customers to take a risk-based approach to managing compliance. In Control Compliance Suite 9.0, we've added Risk Scoring capability that allows a variety of risk-based scoring on the basis of standards, i.e., CIA values and others. The

Solution Overview: Compliance and Security Management Symantec™ Control Compliance Suite 9.0

scoring formula is based on an industry standard Common Vulnerability Scoring System methodology.

- Assess overall risk posture based on:
 - Risk metrics assigned to checks and assets
 - Scoring formula based on CVSS methodology
 - Check metrics (based on vulnerability/exploit potential)
 - Asset metrics (based on asset importance)
-

Enhanced Compliance Reporting

- Dedicated report and dashboard processing subsystem
 - Extensive list of predefined reports and dashboards
 - Ability to distribute reports as e-mail attachments
 - Support for Historical Data Management
-

Enhanced Exception Management

- Centralized exception management
 - Exception templates to address application-specific issues
 - Role-based workflow for segregation of duties
 - Notification sent on state change and prior to expiration
-

Enhancements to Control Compliance Suite applications

- Policy Management—New policy creation wizard, new

mapping interface, enhanced integration, exception management, asset system, policy risk rating, enhanced reports, and dashboards

- Standards Management—Standards-based data collection, composite standards, enhanced check-builder, change auditing, and extended platform support
- Entitlements Management—Entitlement management for databases (Oracle and SQL Server), entitlement change reporting, enhanced reporting, and exception management support for second-level approval
- Response Assessment—Associate the surveys to respondents and assets, attach evidence to the survey response, integration with Control Compliance Suite Asset System quizzing, set threshold values and retries, and scores responses
- Security Information Manager 4.6 is now part of the Control Compliance Suite family
- Service provider architecture support, asset grouping, hierarchical incident creation, and HoneyNet Intelligence Tab

Solution Overview: Compliance and Security Management Symantec™ Control Compliance Suite 9.0

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 providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

Confidence in a connected world.

