

CCS 9.0: A Comprehensive Compliance Management Suite, An Opportunity for Symantec

Date: June, 2008

Author: Jon Oltsik, Senior Analyst and Mary Johnston Turner, Research Analyst

Abstract: Symantec announced a new version of its Control Compliance Suite at its recent Vision event in Las Vegas. What's the big deal? Its new CCS 9.0 may be the most comprehensive compliance suite available today. Since large organizations are clamoring for compliance automation, Symantec may be in a unique position to help these customers, sell CCS, and open the door for other business.

Overview

Amongst the glitter and slice of Americana called Las Vegas, Symantec announced its Symantec Control Compliance Suite (CCS) 9.0 last week. CCS builds on a long heritage of compliance management products from Symantec. Early in the decade, Symantec provided compliance management support as part of its Enterprise Security Manager (ESM) product. To expand its compliance coverage, the company doubled-down on with its 2005 acquisition of industry leader BindView for \$209 million.

There are lots of compliance management products available, but CCS is really positioned as a compliance "manager of managers" – an integrated suite of products providing compliance management services across multiple government/industry regulations and an assortment of technologies distributed throughout a global enterprise. To meet the compliance needs of the world's largest organizations, CCS offers wide-ranging functionality including:

- **Centralized policy management.** Creating, distributing, and managing IT policies seems pedestrian but many IT organizations can't keep up with these seemingly simple policy management tasks. Why? Various regulations demand independent policies while policy approval, distribution, and maintenance can become never-ending manual error-prone processes. CCS can help large organizations overcome these monotonous issues. The product ships with over 125 sample policies and policy templates based upon Symantec's compliance experience and industry best practices. These guidelines help organizations customize and map policies to specific regulations and governance needs. Beyond policy creation, CCS automates workflow associated with policy distribution, end user acceptance, and exceptions. Finally, CCS provides loads of visual dashboard tools and reports, to assess and reacted to policy compliance and violations. CCS also provides centralized control and management of non-programmatic controls thus automating processes that are often based upon paper-based surveys, manual distribution/collection, and physical security safeguards.
- **Data and application-centric views.** In spite of multiple layers of security technologies, many organizations can't easily determine which users have access to specific applications and regulated data. CCS addresses this deficiency through its Entitlement Manager (EM). EM discovers access and authorization permissions from a wide range of systems and data stores across the enterprise. It then translates this techno-babble into human-readable reports for business managers, security administrators, and compliance auditors. Additionally, CCS can help business managers and IT auditors automate the workflow around entitlement approval. This alone can help IT streamline processes; lower operations cost, and avoid costly mistakes.
- **Controls management.** Regulatory compliance depends upon the creation, monitoring, and enforcement of thousands of IT controls. It is hard enough establishing these controls but many organizations have problems detecting and addressing controls violations in a timely manner. CCS helps alleviate these

issues with its Standard Manager. In essence, the Standard Manager delivers a recipe for security best practices for IT assets like servers, databases, and security devices. Standard Manager also integrates with trouble ticketing and CMDBs so that controls violations are corrected quickly following formal change management methodologies.

- **Security integration.** Given its roots, it is no surprise that Symantec stresses a strong linkage between compliance and security. With CCS 9.0, Symantec added to this connection by tightly integrating CCS with its Symantec Security Information Manager (SSIM) 4.1. This helps in several ways. First, SSIM acts as an efficient, high capacity log management services for CCS by collecting, processing, and storing vast amounts of log data for long periods of time. Second, SSIM adds real-time threat detection/remediation capabilities to CCS compliance management capabilities. Finally, CCS and SSIM integration can provide a central workflow and reporting service for IT operations. This can help reduce problem isolation and response time.

CCS has always been one of the few products that can provide these compliance services for large enterprises. With CCS 9.0, Symantec will actually raise its game with a number of attractive additions to its product suite. CCS 9.0 supports policy risk scoring for business alignment. With policy risk scoring, any issue associated with IT assets designated with high risk tags will automatically be prioritized for immediate attention. Symantec also improved CCS usability with a host of new wizards, reports, and templates. Finally, CCS 9.0 provides some technical advances like the integration of Symantec and BindView agent and agent-less data collection and supporting open interfaces like web services and XML data standards easing third-party integration.

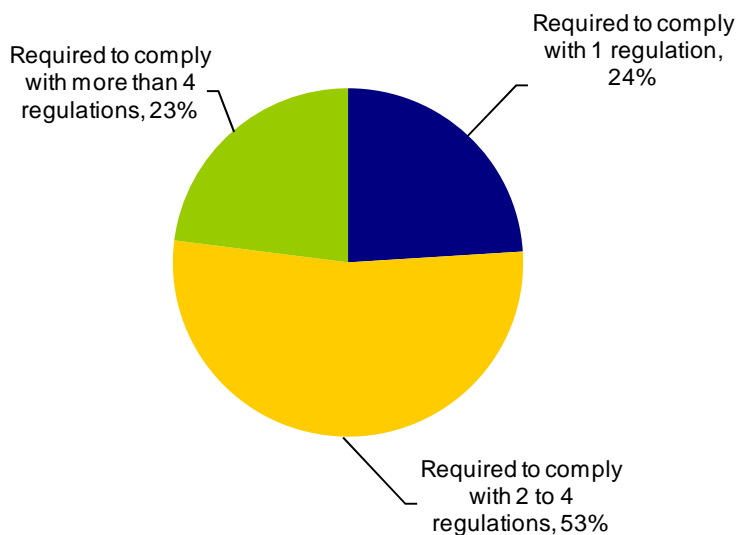
Users Are Crying for Compliance Help

The compliance race has changed radically over the past few years. When regulations like Sarbanes-Oxley and the Payment Card Industry Data Security Standard (PCI DSS) first appeared a few years ago, large organizations had to run at a full sprint to meet regulatory requirements with a fixed deadline. Once these initial obstacles were achieved, regulatory compliance became more analogous to a marathon dependent upon comprehensive processes and consistent performance. Given this new model, Symantec CCS may be especially attractive because large organizations:

- **Juggle multiple simultaneous regulations.** Regulatory compliance is often a multi-layered beast across the enterprise. Why? Large organizations have to comply with multiple regulations each with independent policies, processes, metrics, and audit procedure. ESG Research indicates that the bulk of large organizations must comply with between 2 and 4 regulations while nearly one-fourth of all enterprises have to comply with more than 4 regulations (see Figure 1). Yes, this creates a lot of unavoidable process overlap but without automated tools for compliance management, this situation is often unavoidable. Symantec CCS is designed for this exact type of regulated organization. By centralizing policies, automating data collection and monitoring, and customizing reporting and auditing, CCS can help eliminate compliance redundancy and its associated resource drain.

FIGURE 1. LARGE ORGANIZATION MUST COMPLY WITH MULTIPLE REGULATIONS

Number of regulations organizations are required to comply (Percent of respondents, N=207)

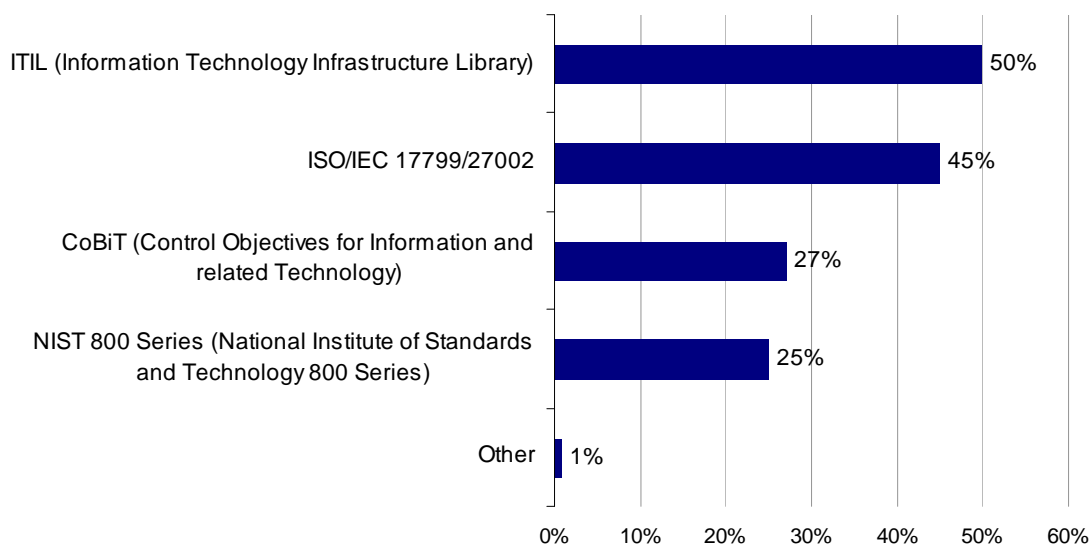


Source: Enterprise Strategy Group, 2007

- **Depend upon IT Service Management as a foundation.** Regulatory compliance demands a more discipline and formal approach to IT governance – one based upon processes, data collection, and metrics. These requirements have driven broad adoption of IT best practice models like the Information Technology Infrastructure Library (ITIL), the International Standards Organization (ISO) 17799/27002 security standards, and the Control Objectives for Information and related Technology (CoBiT) guidelines. ESG Research illustrates this trend, 50% of large organizations have embraced ITIL while many enterprises are utilizing multiple best practice models (see Figure 1). To support these IT service management frameworks, CCS provides policies, data collection, and reporting.

FIGURE 2. LARGE ORGANIZATION ARE EMBRACING IT SERVICE MANAGEMENT FRAMEWORKS

Has your organization implemented any of the following IT governance and security frameworks? (Percent of respondents, N = 207, multiple responses accepted)

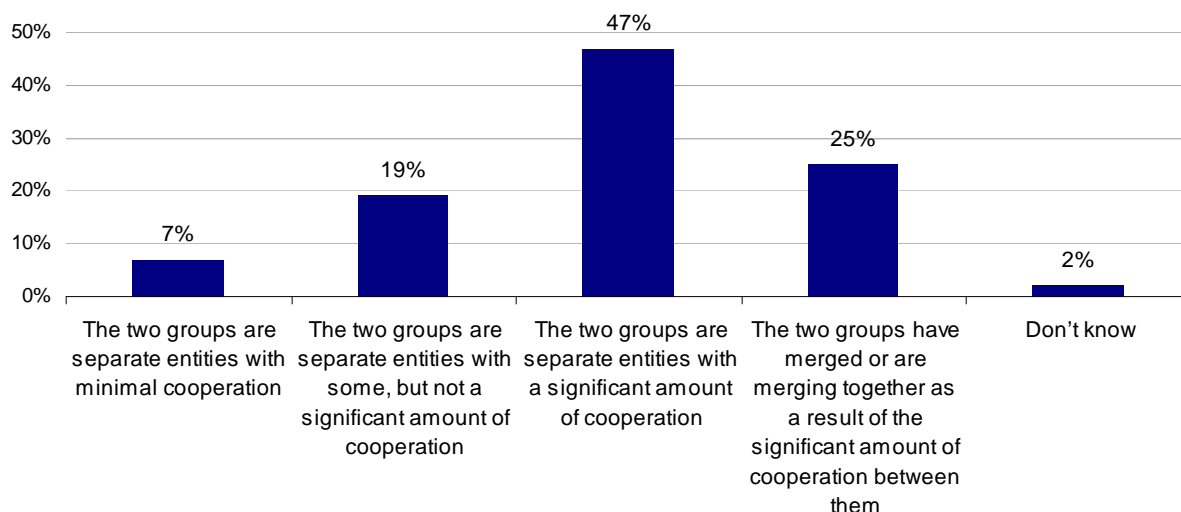


Source: Enterprise Strategy Group, 2007

- Are merging security and compliance organizations.** Compliance was once a separate organizational domain but this is changing. According to ESG Research, these two organizations collaborate often and in some cases are merging into a single group (see Figure 3). By tightly integrating CCS 9.0 with SSIM 4.1, Symantec's compliance product suite closely emulates this organizational change.

FIGURE 3. SIGNIFICANT COOPERATION BETWEEN SECURITY AND COMPLIANCE ORGANIZATIONS

In terms of security management, which of the following statements best describes the way the regulatory compliance and information security groups (or functions) work together in your organization? (Percent of respondents, N = 207)



Source: Enterprise Strategy Group, 2007

Many large organizations complain about a condition they refer to as “compliance fatigue.” With multiple regulations driving a wave of policies, controls, and metrics, enterprises feel like they spend an inordinate amount of time and effort to prepare for each individual audit. Symantec obviously recognizes this. As a central “command-and-control” point for compliance, Symantec CCS should help companies greatly reduce their compliance burden while reducing costs and improving IT productivity in the process.

The Bottom Line

With its enterprise scale and coverage, CCS is a pretty unique product with few competitors. In fact, Symantec’s main competition is likely to come from custom service engagements by the big System Integrators or a network of tactical point tools. Neither solution provides the technical breadth or automation of CCS.

Given this exclusive position, CCS may provide Symantec with a number of other opportunities. For example, CCS may help pull lots of other products like Vontu DLP and Enterprise Vault that can help safeguard and store private data for compliance. Symantec should also utilize CCS strengths to partner with business-centric integrators like Accenture, Ernst & Young, and others to marry business consulting with process automation.

For large organizations, compliance suites like CCS are inevitable. Smart CIOs and compliance officers will evaluate CCS sooner rather than later in order to transform compliance from an on-going nightmare to an automated business process.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.