Managing IT risk and compliance in today’s enterprise is a complex undertaking. IT security leaders find themselves at a crossroads where a growing number of business and regulatory drivers and an evolving threat landscape come together with a staggering array of technology solutions. They need be able to embrace all of these changes, while carefully managing the associated risks.

Critical to their success is the ability to transition from the traditional role of technical expert to business risk advisor. Today’s IT security leaders must be able to clearly communicate the state of their constantly changing environment to a range of different stakeholders – IT operations, audit, and business leaders – in terms that each group can understand and act upon. As security threats and IT risk management become boardroom-level discussions, security leaders must be able to communicate and prioritize their IT risks in business-relevant terms in order to drive change and accountability.

For many organizations, this transition is a challenging one. Their view of IT risk is often generated by multiple point-product solutions, each one providing only a narrow tactical perspective. Bringing together all of the data from these solutions and creating one composite view of IT risk and compliance can be difficult and time-consuming. For organizations who have not yet automated these processes, the challenge is even greater. Their view of IT risk is generally based on subjective manual assessments which often yield inaccurate results that can quickly become obsolete in a rapidly changing environment.
Symantec™ Control Compliance Suite addresses today’s complex IT risk and compliance challenges by providing a solid framework on which to build your IT Governance, Risk, and Compliance program. Control Compliance Suite helps you to communicate IT risk in business-relevant terms, prioritize remediation efforts based on a composite view of risk, and automate assessment processes to improve overall security and compliance posture.

**Connect to the Business**

With more than twelve years of experience assessing IT risks at an asset level, Control Compliance Suite has always provided a rich data set to evaluate an organization’s risk and compliance posture. However, being able to translate this data into actionable insights for business stakeholders is becoming more critical than ever. With the most recent release of Control Compliance Suite, Symantec addresses this issue by providing the ability to create a new view of IT risk as it relates to business process, group, or function.

**Symantec™ Control Compliance Suite Risk Manager** provides the ability to define a virtual business asset which you can manage from an IT risk perspective. This virtual business asset could be your e-commerce site, credit card services group, or transaction processing system. By grouping together all of the IT assets associated with your virtual business asset, you can start to manage the composite risk associated with it. Working with business unit leaders to define risk thresholds up front, you can model the most efficient way to reduce risk in order to meet these thresholds and monitor ongoing progress against your remediation plans. Customizable Web-based dashboards allow you to create different views of IT risk for different audiences, providing the insights needed to drive awareness, accountability, and action.
Prioritize IT Risk

Control Compliance Suite provides a rich, data-driven view of your environment to help better prioritize remediation efforts. Native assessment capabilities automatically evaluate technical and procedural controls, while pre-packaged connectors greatly simplify the process of bringing in external information from both Symantec and non-Symantec products. A unique and highly scalable data framework allows you to normalize and analyze all of this data without having to engage extensive professional services. The output is a ‘composite view’ of your IT risk posture which can be used to more intelligently prioritize remediation efforts.

Consider the following hypothetical example. A core server in your mission-critical billing system has a vulnerability score of five, compared to a score of nine for another server in your less critical inventory system. Based on severity scores alone, you would most likely focus your efforts on the less critical system. However, by generating a composite view of IT risk which looks at both the criticality of the business function or process and the technical severity of the vulnerability, it becomes clear that the vulnerability on your billing system must be addressed first.

Automate Compliance

Automating IT Governance, Risk, and Compliance processes greatly improves your security posture by generating accurate and timely data for faster responses to critical IT issues. Automation can also greatly reduce the cost and complexity associated with meeting multiple compliance requirements.

Control Compliance Suite automates the entire risk and compliance lifecycle from policy and exception management through technical and procedural controls assessment to remediation ticketing. Much of the extra time and effort associated with meeting multiple risk and compliance requirements can come from overlapping controls being measured multiple times for different mandates. Through automation, Control Compliance Suite allows you to measure a given control once and apply that evidence to all mandates for which you need the data, greatly reducing the audit burden on IT Operations. Also, by automatically mapping existing controls to out-of-the-box policy content, you can quickly identify controls gaps in your environment, significantly reducing the time to comply with new mandates or security frameworks.
Control Compliance Suite is an enterprise-class IT Governance, Risk, and Compliance solution comprising a number of different modules with capabilities designed to support the four key stages of a comprehensive IT risk and compliance program; plan, assess, report, and remediate.

**Plan Your IT Risk and Compliance Program**

The planning stage is the foundation for your IT risk and compliance program. From a compliance perspective, it involves creating policies to address multiple mandates, while ensuring these policies are mapped to the appropriate controls in your environment. From a risk management perspective, it involves defining business-centric risk objectives and establishing processes to manage these objectives over time.

Symantec offers the following solutions for the planning stage:

- **Symantec™ Control Compliance Suite Risk Manager** is a new module in our suite which allows you to create a view of IT risk as it relates to a business asset, whether that’s a business process, group, or function. For each business asset you can define business-centric risk objectives, group together all IT assets associated with them, and apply and monitor relevant controls. Working with business unit owners, you can define appropriate risk thresholds and deliver customized Web-based dashboards to monitor how you are doing against these risk thresholds on an ongoing basis. Control Compliance Suite Risk Manager also allows you to model risk reduction over time as scheduled remediation activities take place.

- **Symantec™ Control Compliance Suite Policy Manager** greatly simplifies the process of complying with multiple mandates. It features extensive out-of-the-box policy content in the form of sample policies and policy templates, including regulations and best practice frameworks. These policies are automatically mapped to control statements for both technical and procedural controls, allowing you to assess a control once and use the results across multiple mandates. Policy content and control mappings are automatically updated on a quarterly basis, eliminating the need to engage extensive professional services. Control Compliance Suite Policy Manager also automates the entire IT policy lifecycle from definition, review, and approval to tracking of exceptions and acceptances.
Assess Your IT Environment

The assessment stage centers on the evaluation of performance against desired standards and controls. A true view of IT risk and compliance posture necessitates moving beyond subjective risk assessments which are often error-prone and hard to defend. Instead, combining and analyzing data from multiple different sources across your IT environment establishes a ‘composite view’ of IT risk.

Symantec offers the following solutions for the assessment stage:

- **Symantec™ Control Compliance Suite Standards Manager** is an industry-leading configuration assessment solution, designed to evaluate whether your systems are properly secured, configured, and patched. It offers best-in-class pre-packaged content with over 2,900 control statements mapped to multiple regulations and frameworks. Agent-based and agentless data gathering options facilitate flexible controls evaluation with support for over 100 hardware and software platforms.

- **Symantec™ Control Compliance Suite Vulnerability Manager** delivers end-to-end vulnerability assessment of Web functions, databases, servers, and other network devices. Advanced risk scoring allows you to differentiate between real threats and potential vulnerabilities, ensuring that your most critical and exploitable vulnerabilities are given priority when it comes to remediation efforts.

- **Symantec™ Control Compliance Suite Assessment Manager** simplifies the assessment of procedural controls by replacing costly, time-consuming manual assessments with automated Web-based surveys. It features out-of-the-box coverage for multiple regulations, frameworks, and best practices all translated into questionnaires. Integration with Symantec™ Data Loss Prevention can improve your overall security posture by delivering remedial security awareness training in real-time, based on an immediate need.

At the center of Control Compliance Suite is a unique and highly scalable data framework and controls library which allows you to easily normalize and analyze data from multiple different sources without having to engage extensive professional services. You can combine rich, native assessment data from Control Compliance Suite with data from other Symantec and non-Symantec sources, collected by pre-packaged connectors. By normalizing this data, you can see a multitude of data points associated with a given control, for a truly ‘composite view’ of your IT risk posture.
Report on IT Risk and Compliance Posture

In order to drive awareness, accountability, and action, reporting needs to look beyond vulnerabilities or configuration issues for individual assets. Instead, it must provide the ability to look at all assets which make up critical business entities and clearly communicate IT risk and compliance posture across these assets in a way that makes sense to multiple different stakeholders.

Leveraging the ability to aggregate and normalize data from multiple different sources, Control Compliance Suite pulls from its scalable data framework to generate dynamic **Web-based dashboards and reports** for multiple audiences. These dashboards can be used to communicate current risk exposure, illustrate how risk levels are trending over time, and model the impact of planned remediation activities. Because dashboards are customizable, you can deliver targeted views and metrics for different audiences. For example, a CIO could view the risk level of the online e-commerce store or overall PCI compliance for the business. A business unit owner could view risk scores for their online banking system and monitor how those scores are trending over time. A Director of IT Operations could drill down deeper to analyze the data behind a particular risk score while planning remediation activities and monitoring results over time.
Remediate Based on Highest Priority Risks

Given the complexity of today’s IT environments and the lack of sufficient resources, being able to prioritize remediation efforts is essential. Ideally you want to use a risk lens to prioritize what needs to be fixed first, be able to automate the process of kicking off remediation tickets, and then have closed-loop remediation to confirm issues have been resolved. Equally important is the risk acceptance process; being able to acknowledge which risks you are not going to address either because there are mitigating controls in place or because these risks are of lower priority to the business.

Control Compliance Suite leverages Symantec Workflow to automate remediation ticketing for popular systems including HP Service Manager™, Remedy™ and Symantec™ Service Desk. Once a control failure is detected, a remediation ticket can be automatically generated with detailed guidelines on how to fix the problem for faster response times. Out-of-the-box integration with the Symantec Service Desk solution facilitates closed-loop remediation, whereby assets are automatically reassessed once the ticket is closed to confirm that the necessary changes were made.

Control Compliance Suite also helps you to prioritize remediation efforts based on risk. Using industry standard risk-scoring algorithms, you can assign a risk score to assets, policies checks, and survey questions. As all of this data is gathered together via our scalable data framework and plugged into reports and dashboards, allowing you to leverage these risk scores to help identify highest priority risks.

Confidence in a connected world. Symantec
Visit our website
www.symantec.com/business/control-compliance-suite

For information on training, visit
www.symantec.com/business/theme.jsp?themeid=ccs_training

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 website.

About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, California, Symantec has operations in 40 countries. More information is available at www.symantec.com