

# Control Compliance Suite Vendor Risk Manager

Continuously Assess, Monitor, & Secure Your Information Supply Chain and Data Center

## Data Sheet: Security Management

### Overview

Enterprise data centers today have increasingly fluid perimeter security infrastructures.

- Many businesses rely on third parties to enable some of their most critical business activities. These partners and vendors often access sensitive business data such as customer and employee personally protected data (PII and PHI) and confidential intellectual property.
- These partners, in turn, may also be sharing sensitive information and critical processes with their own third parties and business partners.
- In addition, enterprises today are increasingly using public cloud and third-party collocation facilities to augment their on-premise data center resources.

An organization may have stringent data security practices in place, but their suppliers and business partners may not exercise the same due care. Malicious entities are very much aware of these potential weaknesses in a business's information supply chain and are constantly looking for ways to exploit these security gaps. Regulatory and legal standards have made it quite clear that outsourcing processes and infrastructure does not transfer risks to the service providers.

security and compliance managers the ability to understand the risks associated with its partner and supplier ecosystems. Symantec Control Compliance Suite Vendor Risk Manager automates many of the tasks associated with the vendor security risk management process, including variable scoping and tiering of vendors, creating assessments and standards and/or mandate-based reports, vendor response tracking and reminders, evidence collection, evidence risk analysis, email notifications to stakeholders, and scheduling. Symantec Control Compliance Suite Vendor Risk Manager provides an inventory of third parties (services and applications) and a catalog of third-party security risks. Customers are able to segment their vendors according to the criticality of the business processes, technology, and IT services they provide and according to the security profile of the information that they access or manage.

Rule-based security assessments are designed so that the most critical and high-risk tiers have the most rigorous evaluations. The solution manages each vendor independently, offering customers the ability to understand the impact of doing business with each contributor in their information supply chain. The combination of procedural and application security assessments enables a more comprehensive view of the third party's relevant security and compliance posture.

Included in this solution are the Symantec Control Compliance Suite Vendor Risk Manager Administrative Console, the Symantec Control Compliance Suite Vendor Risk Manager Relationship Gateway, the Symantec Control Compliance Suite framework, and assessment content from Shared Assessments. To learn more about the complete suite, visit <http://www.symantec.com/control-compliance-suite>



Symantec Control Compliance Suite Vendor Risk Manager (Symantec CCS VRM) delivers the technology that enables

### Is your organization able to:

- Demonstrate an effective vendor security risk management program to your auditors, regulators, and customers?
- Assess the application security posture of third-party applications and IT services that are being used by your organization, including private, hybrid, and public cloud infrastructures?
- View the dependencies and assess IT security risks across multiple vendor, software, and service provider/IT outsourcing relationships across your information supply chain?
- Provide mandate-based reporting on third-party security compliance requirements such as PCI DSS 3, HIPAA Omnibus, CFPB, and OCC Guidelines?
- Automate best practices for the secure onboarding of business partners and suppliers in your information supply chain ecosystem?

### What's New in Control Compliance Suite Vendor Risk Manager 11.1?

- **VRM Dashboards** – New VRM dashboards allow VRM administrators to drill down and filter larger datasets. VRM dashboards are available for the following categories: Overview, Risk Management, and Workflow.
- **VRM Risk Score Cache** – In-memory caching of VRM Risk scores to improve UI responsiveness and facilitate faster dashboard loading for very large data sets.
- **VRM Scheduler Service** – The scheduler service is responsible for all scheduled VRM job management.
- **Support for Prevalent Vendor Threat Monitor**. Integration with VTM enhances VTM visualization for risk and event data in the vendor tab.
- **Survey Editor** – OCIL 2.0 based survey editor is available in VRM Console and allows VRM administrators to create, modify, and test surveys before assigning to evidence sources. Survey editor supports import of OCIL 2.0 surveys as well as custom extensions to the OCIL schema for risk scoring and VRM risk areas. Surveys can also be exported to OCIL (XML), Excel, and synchronized with CCS AM.

- **Flex Form Evidence Source** – the Flex Form evidence source allows VRM administrators to define specific forms and fields for evidence collection and review. Field types are define and input is assign to task assignee or risk reviewer. This is effective for document and contract management.
- **Summary and Detailed Assessment Reports** – VRM administrators can generate summary and detailed reports for a VRM assessment. The report contains scope, risk, evidence, and review details about assessment.
- **RACI Graph** – implemented a RACI graph for relationship responsibilities and activities. This allows VRM administrators the ability to understand who is responsible for activities related to a relationship.
- **Extended Language Support** – added Console and Gateway UI language support for German, French, Spanish, Portuguese, Korean, Traditional Chinese, Simplified Chinese, and Russian.

### Standard Features

Control Compliance Suite Vendor Risk Manager enables you manage the risks posed by your third party business process services, application developers, and cloud service providers by automating security and compliance assessments:

- Leverage Shared Assessments content for controls-based security risks assessment of third parties.
- Deploy a centralized, Web-based repository to manage the vendor assessment process and collection of evidence data.
- Display evidence requests and the status of those requests in a single management interface.
- Enable third-party providers to route requests to appropriate process, data, and system custodians within the vendor organization.
- Enable variable scoping, thus allowing the customer to scope/add multiple vendors, software, and service solutions into a single relationship assessment.

- Auto-calculate vendor risk scores based on multiple evidence sources, and enhance risk scoring by enabling risk weighting by risk areas.
- Integrate with the rest of the Control Compliance Suite applications to offer advanced compliance reporting, dashboards, and analytics, which customers can utilize to support risk remediation, operational alignment, and business planning activities.
- Create and evaluate vendors based on tiers as defined by their importance and potential risk to the organization.
- Provide industry-standard SCAP OCIL 2.0 questionnaire support.
- Integrate directly with Veracode to automate third-party application scanning of application developers and cloud service providers. Application providers are able to upload scan results directly from Veracode via the Symantec Control Compliance Suite Vendor Risk Manager Relationship Gateway. Customers can also manually upload application security reports based on their application security program.
- Support regulatory requirements for vendor monitoring, and better identify potential risks before they become legal liabilities to the business.
- Receive notifications of potential data breaches without being dependent on your third-parties.
- Clearly communicate accurate and up-to-date vendor risk information to executives on short notice.
- Realize operational efficiencies and scale your vendor risk management program.
- Leverage this evidence-based approach to enable more informed business decisions during the vendor selection process.
- Leverage vendor risk assessment information to facilitate internal cross-functional collaboration and manage third-party related incidents.
- Employ vendor risk information to create internal security checklists for on- and off-boarding third party business partners.
- Support internal processes and standards for addressing and responding to third party data breaches.
- Leverage variable scoping to view and assess risks for individual relationships, as well as assess risks across the entire information supply ecosystem.

### Customer Benefits

Control Compliance Suite Vendor Risk Manager offers the following customer benefits:

- Identify and assess the risks posed by your suppliers and business partners to the enterprise's cybersecurity and data center security operations.
- Demonstrate an effective vendor risk management program to your auditors, regulators, and customers.
- Enhance the ability to monitor your risk posture by continuously assessing your third party service provider's relevant IT security policies, procedures, and web application security.
- Support planned third party cloud and software-defined data center migration by providing a hub for conducting due diligence on the security and compliance standards of cloud service providers, managed service providers, and third party application developers.

### Additional Symantec solutions for IT risk and compliance

Control Compliance Suite provides a solid framework on which to build your IT Governance, Risk, and Compliance program. You can communicate IT risk in business-relevant terms, prioritize remediation efforts based on risk, and automate time-consuming manual processes to improve your overall security and compliance posture.

Control Compliance Suite is a modular solution, comprising of five key components which are fully interoperable and available separately or as part of the broader suite. Key infrastructure capabilities available with all modules include a unique and highly scalable data framework to normalize and analyze large volumes of data, customizable Web-based dashboards and reports, and workflow integration with remediation ticketing systems.

**Symantec™ Control Compliance Suite Standards Manager** is an industry-leading configuration assessment solution, designed to evaluate if systems are secured, configured and patched according to standards.

**Symantec™ Control Compliance Suite Risk Manager** conveys the impact of IT risk in business-relevant terms. You can work with business leaders to identify IT risk thresholds, assign ownership, and track risk reduction over time.

**Symantec™ Control Compliance Suite Policy Manager** simplifies policy management with out-of-the-box policy content for multiple mandates, automatically mapped to controls and updated on a quarterly basis.

**Symantec™ Control Compliance Suite Vendor Risk Manager** allows you to gain visibility into your vendor risk exposures to safeguard your sensitive data and reduce overall business risk.

---

### More Information

*Visit our website*

<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 website.

### About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at [www.symantec.com](http://www.symantec.com) or by connecting with Symantec at [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).

### Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

[www.symantec.com](http://www.symantec.com)