If your organization handles payments for major credit cards, demonstrating compliance with the Payment Card Industry Data Security Standard’s (PCI DSS) rigorous mandates can be challenging. In fact, 71% of organizations fail their interim PCI compliance assessment, and only 28.6% of organizations remained fully PCI compliant less than a year after a successful PCI validation.\(^1\) And for many organizations, the motivation to secure your cardholders’ data isn’t just to satisfy PCI compliance, it’s also to avoid being the next headline-grabbing victim of a data breach.\(^2\)

Many organizations rely on Symantec Control Compliance Suite for PCI DSS risk-prioritized security and compliance, continuous assessments, and a unified view of their security controls and vulnerabilities. Control Compliance Suite helps you understand exactly where you do (and don’t) comply with PCI DSS’s requirements so you’re ready for the next audit, and you can quickly create reports to assure executive management your organization is compliant with PCI DSS.

**Why It’s Tough to Get a Complete Picture of Your Compliance**

Addressing the challenges associated with becoming PCI DSS compliance are critical in order to demonstrate your organization truly is complying with the regulations. Many organizations struggle with these common challenges:

**Challenge #1: Gathering both technical and procedural control data.**

One of the greatest challenges in becoming PCI DSS compliant is demonstrating compliance – proving that you’re actually satisfying PCI DSS’s many requirements and having the data to back it up when auditors visit. This type of information needs to be collected for both PCI DSS’s technical and procedural controls. Many compliance solutions just address one type of control but not both. This limitation creates more manual work as you’ll need to gather the missing data and makes it much harder to understand if there are gaps in your security and compliance status.

**Challenge #2: Assessing and reporting on the security status of third-party controls.**

Most organizations that take credit card payments have multiple third-party technologies they use to support these systems, such as point of sale (POS) systems and/or software. These third-party systems also need to be included in your PCI DSS assessments to ensure they have the proper security configurations, but it can difficult and time-consuming to gather without an automated solution.

**Challenge #3: Preparing for audits is time-consuming.**

Having the proper information ready when an auditor visits is crucial. If you can’t quickly run reports to give the auditor the information they need, your team will spend enormous amounts of time chasing data, massaging it, and formatting reports.

---

1 - “Tackling Top Regulation Compliance Challenges,” SearchCompliance, TechTarget, June, 30 2016.
Achieve PCI DSS Compliance with Symantec Control Compliance Suite

You’ll also want the ability to assess your PCI DSS compliance posture at regular intervals so you can identify security gaps and address them before the next audit.

How Control Compliance Suite Helps You Attain PCI DSS Compliance

A software solution alone can’t make you compliant – it’s your processes and properly secured assets that ensure PCI DSS compliance. But using a solution like Symantec Control Compliance Suite to assess security and compliance can make attaining and maintaining compliance a much easier and faster process.

Symantec Control Compliance Suite combines both procedural and technical controls information to help demonstrate PCI DSS security and compliance including:

- Supporting end-to-end automation of internal and external assessments of procedural, technical, and third-party controls
- Generating audit-ready reports and dashboards
- Calculating and aggregating risk scores according to your business’ unique thresholds.

End-to-end automation for technical and procedural controls

Proving PCI DSS compliance requires collecting and maintaining an enormous amount of data about the controls in your environment. Control Compliance Suite automates assessments of technical controls that require secure configuration settings by using network and asset discovery – including for third-party systems such as POS.

By automating IT infrastructure assessments, you can quickly identify misconfigured assets and prioritize issues for remediation. If a technical asset requires attention that affects your compliance status, such as a laptop requiring a configuration setting change or security update, Control Compliance Suite will list the prioritized issue in a remediation report so you can take appropriate action. It even integrates with Symantec ServiceDesk and third-party service desk tools so your helpdesk can be automatically notified when an issue requires their attention.

Procedural controls are also automatically assessed, so you can answer one of the most difficult questions about compliance which is “What’s missing?” Control Compliance Suite helps you pinpoint gaps in your procedural controls with out-of-the-box support for PCI DSS regulations and standards that are translated into policies and questionnaires. You can use these questionnaires to assess the effectiveness of your procedural security controls, evaluate overall employee security awareness, and support security awareness training.

Centrally collect and manage evidence

Control Compliance Suite can combine evidence from multiple sources, including other solutions such as Symantec Data Loss Prevention or your Vulnerability Scanning solution, so you have a complete view of your compliance posture. The evidence that Control Compliance Suite collects is formatted appropriately and mapped to controls which are linked to PCI DSS policies and regulations.

Many organizations that need to comply with PCI DSS also have multiple mandates to satisfy, such as HIPAA, ISO 27001 or ISO 27002. Control Compliance Suite supports over 100+ regulations out-of-the-box so you can assess your technical and procedural controls status once and utilize that information to report on multiple mandates without repeating work.
Audit-ready reports and dashboards to understand your security, compliance, and risk posture

Now you can create reports at a moment’s notice to prepare for an audit – no more digging through data or massaging it into the appropriate format that PCI DSS auditors prefer. Control Compliance Suite gives you a holistic view with customizable, multi-level reports for PCI DSS-based mandate reporting that combine both Control Compliance Suite and third-party data.

Dynamic dashboards show your overall PCI DSS compliance status so you can focus on your biggest priorities. If an auditor requests that you create a prioritized response plan, use Control Compliance Suite’s risk-ranked results to help determine which risks pose the biggest threats and should be included in your plan. You can also setup role-based viewing for reports and dashboards so users view just the information that’s appropriate for them. You can even give auditors access to specific reports while you maintain control over the information that they can access and view.

![Control Compliance Suite Dashboard](image)

Figure 1: All controls are configurable in Control Compliance Suite and each control statement can be mapped to the appropriate PCI DSS mandate.
Figure 2: Procedural assessment questions are mapped to controls in Control Compliance Suite.

Figure 3: You can easily assess compliance for multiple mandates and overall compliance for all organizational controls.
Figure 4: Reports and dashboards help you quickly assess your overall compliance.
Next Steps

Take the next step in learning how Control Compliance Suite can enable your PCI DSS compliance program and give you a unified view of your security controls and vulnerabilities. Learn More

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

11/16 Part #21370383