ControlScan

PCI DSS Compliance Solutions

Designed for the unique needs of small and mid-sized businesses

What's the point of PCI compliance?

The Payment Card Industry (PCI) Security Standards Council (an organization formed by the card brands) created the PCI Data Security Standard (DSS) to ensure that businesses follow best practices for protecting their customers' payment card information.

The same technologies that make everyday business efficient also make it easy for hackers to access sensitive information. That's why a business taking "just a handful" of credit cards is no less obligated to protect that card data than the major retailer running thousands of transactions.

When fully and accurately implemented, the 12 requirements of the PCI DSS work together to provide your business with defense-in-depth; that is, multiple layers of security that make it much more difficult for an attacker to gain access to your customers' payment card data. Studies have shown that cyber thieves and their automated tools most often seek out basic mistakes such as weak passwords, misconfigured technologies and uneducated employees. The PCI DSS addresses these and other areas of weakness to effectively shield your business.

PCI is a big deal for small business. We make it easy.

ControlScan recognizes that security and compliance go hand-in-hand. As a result, we offer a suite of security solutions that help you achieve PCI DSS compliance and improve your overall security posture. We also employ a team of security experts to provide guidance on your layered, security defense strategy and answer any questions that you may have.

The following table maps the PCI DSS requirements to the ControlScan security solution and/or service that can help you satisfy the requirement. We encourage you to contact our team of security and compliance experts if you have any questions about these services or how to achieve compliance.

PCI DSS 3.x Requirements	PCI Requirement Addressed	Solution/ Service Needed to Satisfy	ControlScan PCI DSS Compliance Solutions that satisfy the requirements
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1, 1.2 and 1.3	Unified Threat Management Firewall	Unified Threat Management Firewall (UTM Firewall) provides continuous network monitoring and protection against outside threats, including intrusion detection and prevention. When in place, this solution can help you meet requirements 1.1, 1.2 and 1.3.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	4.1	SSL Certificates	Secure Socket Layer (SSL) Certificates assure site visitors that your site is protected. ControlScan offers the benefit of cost savings on SSL certificates from well-known, trusted certificate authorities. This solution satisfies requirement 4.1 when implemented with secure transport layer protocols (HTTPS/TLS 1.2).
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	5.1, 5.2, 5.3	Advanced Endpoint Security	Advanced Endpoint Security services include traditional (signature-based) and next-generation (analytics-based) malware protection, with frequent updates and real-time lookup. This solution can be used to satisfy requirements 5.1, 5.2, and 5.3.
Requirement 6: Develop and maintain secure systems and applications	6. 2, 6.6, 11.3	Web Application Security Testing Web Application Firewall (Web Security Services)	Web Application Security Testing services simulate attacks against your applications (e.g., web-based, API) to identify threats and vulnerabilities resulting from insecure code. This solution can be used to satisfy requirement 6.6 as well as the application level testing required by 11.3. Web Security Services, including a Web Application Firewall, address new threats and vulnerabilities on an ongoing basis, and ensure these applications are protected against known attacks. This solution can be used to satisfy requirement 6.6.
Requirement 10: Track and monitor all access to network resources and cardholder data	10.5, 10.6, 10.7	Log Monitoring and Management	Log Monitoring and Management collects log and machine data for analysis. Information is correlated and reviewed to identify anomalies of suspicious activity on a continuous basis. The log monitoring service provides real time alerts on possible unauthorized access to the cardholder data environment and other critical systems. Collected data is archived within secure storage for later reference. This service helps meet requirements 10.5, 10.6, and 10.7.

PCI DSS 3.x Requirements	PCI Requirement Addressed	Solution/ Service Needed to Satisfy	ControlScan PCI DSS Compliance Solutions that satisfy the requirements
Requirement 11: Regularly test security systems and processes	11.1, 11.2, 11.3, 11.4, 11.5	Internal Vulnerability Scanning	Internal Vulnerability Scanning identifies vulnerabilities within your internal systems so that you can harden them against attack. This solution satisfies requirement 11.2.1.
		PCI External Vulnerability Scanning	SmartScan PCI External Vulnerability Scanning checks for cross-site scripting, SQL injection, remote file inclusion and other application and network-based vulnerabilities. This solution satisfies requirement 11.2.2.
		Network and Application Penetration Testing	Network and Application Penetration Testing services simulate attacks against your critical information systems and applications. These services are delivered by our staff of veteran penetration testers. These services satisfy requirements 11.3, 11.3.1 and 11.3.2.
		Network Segmentation	Applicable for those qualifying for SAQ C, Segmentation Validation is an alternative to a full penetration test that validates effective network segmentation. This solution is available to those utilizing the ControlScan UTM Firewall service and addresses requirement 11.3.4.
		Network Intrusion Detection	Network Intrusion Detection capabilities built into our UTM Firewall solution help to alert you of anomalous activity on your networks. This will help satisfy requirement 11.4.
		File Integrity Monitoring	File Integrity Monitoring (FIM) satisfies requirement 11.5, which requires file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
		Host Intrusion Prevention	Advanced Endpoint Security includes Host-based intrusion prevention which helps further complete requirement 11.4 for workstations and servers.
Requirement 12: Maintain a policy that addresses information security for all personnel	12.1, 12.2, 12.3, 12.6, and 12.10	Policy Builder	Policy Builder provides you the opportunity to generate a baseline set of policies to help with PCI compliance. Policies required throughout the entire PCI DSS are available, including the Information Security Policy, Acceptable Use Policy, Security Awareness Training Policy and Incident Response Plan Policy required by 12.1, 12.3, 12.6, and 12.10 respectively.
		IT Risk Assessment	The ControlScan Security Consulting team conducts IT Risk Assessments that evaluate your most critical IT assets and functional areas to determine the impact a malicious act or loss of data would have on your organization's operations. This solution satisfies PCI requirement 12.2.
		Security Awareness Training	PCI Security Awareness Training offers comprehensive courses to educate your employees on the critical areas of vulnerability and security best practices. This cloud-based tool provides on-demand reporting capabilities allowing you to track user progress and completion and assign courses quickly and effectively. This solution satisfies requirement 12.6.

For more information about any of our services, or to receive a complimentary assessment of your current security and compliance posture, give us a call at 800-825-3301 x 2 or visit www.controlscan.com.

We've got your back.

About ControlScan

ControlScan is the Managed Security Service Provider with a difference: We take a proactive approach to protecting businesses from cyber threats while helping ensure their compliance with security and privacy standards like PCI DSS and HIPAA/HITECH. Our unified security and compliance services deliver confidence to millions of businesses as well as the IT professionals who serve them. Merchant service providers and web hosting companies also partner with us to reduce cybercrime-related business risk. Based in Atlanta, ControlScan is venture backed and supported by a worldwide base of customers, partners and strategic alliances.