



What Is the Payment Card Industry Data Security Standard?

The Payment Card Industry (PCI) Data Security Standard (DSS) applies to all businesses, large and small, in any industry that processes, transmits, or stores credit card transactions and cardholder information. The goal of the PCI DSS is to increase protection of credit card information and related transactions. PCI DSS Version 2.0 was released in October 2010 and goes into effect in January 2011, and includes clarifications and additional guidance to provide more clarity to the existing PCI standards. PCI DSS emphasizes network segmentation to determine the PCI scope and cardholder data environment, and outlines sampling size determination for organizations during an audit.

PCI Deadlines and Enforcement

MasterCard was the first to release global PCI DSS deadlines and non-compliance fines. Organizations must achieve PCI DSS 2.0 compliance by December 31, 2011. Level 1 and Level 2 merchants must have an external audit performed by a PCI Qualified Security Assessor (QSA) to achieve PCI DSS compliance. Level 3 merchants can perform internal audits to meet PCI DSS compliance. MasterCard defines the merchant levels as outlined below.

PCI Level	Transaction Volume	Validation Requirements
LEVEL 1	Process more than 6 million MasterCard (or VISA, AMEX, JCB, or Discover) transactions annually Any company that has suffered a credit card breach in the last 12 months	Annual onsite audit by Qualified Security Assessor (QSA) Quarterly network scan by Approved Scan Vendor (ASV)
LEVEL 2	Process 1 million to 6 million MasterCard (or other card brand listed above) transactions annually	Annual onsite audit at merchant's discretion Quarterly network scan by ASV Annual self-assessment questionnaire signed by officer of company

PCI Level	Transaction Volume	Validation Requirements
LEVEL 3	Process 20,000 to 1 million e-commerce transactions annually	Quarterly network scan by ASV Annual self-assessment questionnaire signed by officer of company
LEVEL 4	All other merchants	Annual self-assessment questionnaire signed by officer of company

MasterCard reclassifies the service provider levels so that Level 1 service providers include all third-party processors (TPPs) and data storage entities (DSEs) with more than 300,000 annual transactions. Level 2 service providers are all DSEs with fewer than 300,000 annual transactions.

MasterCard also defines PCI DSS noncompliance assessment structure for Level 1, 2, and 3 merchants. This is for PCI DSS noncompliance only, not assessment resulting from a breach.

Noncompliance Assessment Structure Per Calendar Year		
Organization	Assessment Amount (USD)	Occurrence
Level 1 and 2 Merchants	Up to \$25,000 Up to \$50,000 Up to \$100,000 Up to \$200,000	First violation Second violation Third violation Fourth violation
Level 3 Merchants	Up to \$10,000 Up to \$20,000 Up to \$40,000 Up to \$80,000	First violation Second violation Third violation Fourth violation
Level 1 and 2 Service Providers	Up to \$25,000 Up to \$50,000 Up to \$100,000 Up to \$200,000	First violation Second violation Third violation Fourth violation

The PCI DSS standard provides 12 security requirements that companies must adhere to:

1	Install and maintain a firewall configuration to protect data.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.
3	Protect stored data.
4	Encrypt transmission of cardholder data and sensitive information across public networks.
5	Use and regularly update antivirus software.
6	Develop and maintain secure systems and applications.
7	Restrict access to data by business need-to-know.
8	Assign a unique ID to each person with computer access.
9	Restrict physical access to cardholder data.
10	Track and monitor all access to network resources and cardholder data.
11	Regularly test security systems and processes.
12	Maintain a policy that addresses information security.



Cisco Solutions for PCI

Cisco offers numerous technology solutions and advanced services to help companies address their PCI DSS requirements. Because PCI covers many parts of the network, no single product or technology meets all of the PCI technology requirements. The following lists Cisco products and technologies that help to address PCI requirements.

Routers and Switches	Security	Wireless	Data Center	Management	Services
<ul style="list-style-type: none"> • Cisco® Integrated Services Routers (ISRs) • Cisco Aggregation Services Routers (ASRs) • Cisco Catalyst® Series Switches 	<ul style="list-style-type: none"> • Firewall: Cisco ASA 5500; Cisco ISRs and ASRs, Cisco Catalyst 6500 Series Switches • Intrusion Prevention System: IPS 4200 and IOS® Software modules • VPN: IPsec and SSL VPN, GET VPN, DMVPN • Cisco Video Surveillance solutions • Network Admission Control (NAC): appliance, ISR module, and NAC Profiler • IronPort® Series Email Security Appliance 	<ul style="list-style-type: none"> • Cisco Unified Wireless Network Solution • Cisco Aironet® 1100 and 1200 Series Access Points • Cisco Wireless LAN Controller (appliance and ISR module) • Cisco 3300 Series Mobility Services Engine • Cisco Wireless Control System (WCS) • Cisco Adaptive Wireless IPS (wIPS) • Wireless scanning and monitoring 	<ul style="list-style-type: none"> • Cisco Nexus® 7000 Series Switches • Cisco Nexus 1000V Series Switches • Cisco MDS with Storage Media Encryption (SME) module • Cisco Unified Computing System (UCS) • Cisco Wide Area Application Services (WAAS) Appliances and ISR Network Module 	<ul style="list-style-type: none"> • Cisco Security Manager • CiscoWorks LAN Management Solution • Cisco IronPort M-Series Appliance • Cisco SIEM Partners • Cisco Secure Access Control System (ACS) • Cisco Wireless Control System (WCS) 	<ul style="list-style-type: none"> • IT GRC Services • Network Segmentation Advanced Services • Interactive Voice Response Service through Cisco Unified Customer Voice Portal

Cisco® Validated Designs are another critical element of Cisco’s PCI solution portfolio. Built and tested in Cisco labs, these designs have been evaluated by a PCI QSA, who then provided a report on compliance (ROC) outlining how each solution addresses PCI DSS technology requirements. The Cisco Validated Designs for PCI can be downloaded from <http://www.cisco.com/go/pci>. The independent ROCs for Cisco’s PCI solutions are also available for viewing at this address.

What Are the Benefits of Cisco Solutions for PCI?

Cisco PCI solutions address many of the 12 PCI DSS requirements. They go beyond just the requirements—for example, with newer technologies such as virtualization—and provide comprehensive best practices for securing sensitive information. Cisco PCI solutions can strengthen a company’s overall security posture and help customers satisfy their PCI DSS requirements in a cost-effective and efficient manner.

Cisco Validated Architectures are a set of PCI-audited designs that aid customers in designing and implementing networks that meet PCI DSS requirements. These architecture designs offer guidance for remote location, Internet edge, and data center networks, with the independent ROC available for customers to review.

For More Information

For more information on Cisco PCI solutions, please visit <http://www.cisco.com/go/pci>, <http://www.cisco.com/go/retail>, or <http://www.cisco.com/go/healthcare>.