

IT Security & Privacy Practice

Payment Card Industry Data Security Standards (PCI
DSS)
Compliance Services | FAQ

August 20, 2008

Ron Schmittling, CPA.CITP, CISA, CIA

rschmittling@bswllc.com | 314.983.1398

1050 N. Lindbergh Blvd | St. Louis, Missouri 63132
1551 Wall St. | St. Charles, Missouri 63303
314.983.1200 | 888.279.2792
www.bswllc.com



IT Security & Privacy Services

Information Security	Payment Card Risk	Cybercrime & Incident Response	Information Privacy & Data Protection	Information Security Compliance
<ul style="list-style-type: none"> ■ Security Risk Assessments ■ External Network Penetration Studies ■ Internal Network Vulnerability Assessments ■ Network Security Controls Reviews ■ Wireless Security ■ Web Application Security & Pen Tests ■ CISO as you Grow ■ Social Engineering ■ SMB Security Reviews ■ VOIP Assessments 	<ul style="list-style-type: none"> ■ PCI Compliance GAP Assessments ■ PCI Merchant Compliance Services ■ PCI Card Processor Compliance Reviews ■ PCI Data Hosting Provider Compliance ■ ATM Network Compliance ■ TG-3 Network Security Reviews for STAR, NYCE and Pulse ATM networks 	<ul style="list-style-type: none"> ■ Digital Forensics – Non-Litigation Services ■ Digital Forensics – Litigation Support Services ■ Electronic Data Discovery Planning, Analysis, Timeline Construction, and Damage Assessment ■ Email Extraction and Reconstruction ■ Data Recovery ■ Expert Testimony ■ Incident Response GAP Assessment ■ Incident Response Strategy, Design & Implementation ■ Emergency Incident Response Team 	<ul style="list-style-type: none"> ■ Data Privacy Services (AICPA Certification) ■ Data Privacy Compliance (Industry, Federal & State) ■ ID Theft Prevention and Response ■ Data Protection GAP Assessments ■ Data Protection Strategy, Design and Implementation 	<ul style="list-style-type: none"> ■ Attestation/Agreed Upon Procedures ■ HIPAA Privacy and Security ■ ISO 17799, 27001, 27002 Assessments ■ FFIEC Security Assessments and Compliance ■ SOX Security Readiness and Testing ■ FDIC Reviews ■ GLBA Assessments ■ ITIL Standard Reviews ■ WebTrust & SysTrust Certifications



OVERVIEW | PCI Compliance

WHAT	Security standards created to protect customers from identity theft and security breaches. Noncompliance results in fines and other penalties.
WHO	<u>Any</u> company that accepts, processes, or stores credit card information needs to comply with PCI.
WHERE/ HOW	Security Assessment Performed onsite (Tier 1) or remotely (Tier 2, 3, 4) Network Scan Performed remotely for external facing IP addresses involved in the credit card process (accept, transmit, store); Done on a quarterly basis Reporting Successful compliance reports are sent to the merchant's bank.
WHEN	Compliance regulations are enforceable NOW!



FAQ

- **What is Payment Card Industry (PCI) Compliance?**
PCI Compliance is a set of security standards that were created by the major credit card companies (American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International) to protect their customers from increasing identity theft and security breaches.
- **Do I need to become compliant?**
Any company that accepts, processes, or stores credit card information needs to comply with the standards set by PCI.
- **What kind of a scan needs to be performed?**
Network vulnerability scans must be performed by PCI Approved Scanning Vendors (ASV). The scan will be performed over all externally facing IP addresses that touch the credit card acceptance, transmission and storage process.
- **What if a vulnerability is found during a scan?**
If a level 3,4 or 5 vulnerability is found during a PCI Scan, the company will not receive a passing PCI Scan report.



FAQ (cont'd)

- **How long does it take to become compliant?**
The PCI compliance process can take anywhere from one day to two weeks. The amount of time it takes for a company to be considered compliant is dependent on the threats the PCI scan discovers and the amount of time it takes to complete the self assessment questionnaire.
- **How do I report compliance?**
Both the passing PCI scan and annual assessment materials should be turned into your merchant bank. Your merchant bank will then report back to PCI that your company is PCI Compliant.
- **What happens if I am not compliant?**
Failure to comply with the PCI security standards may result in heavy fines, restrictions or permanent expulsion from card acceptance programs.

PCI Standards

- **PCI compliance and validation regulations apply to *financial institutions, Internet vendors and retail merchants.***

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security