

## ▶ Payment Card Industry Data Security Standard

Compliance Overview  
by Brad C. Johnson and Philip C. Cox

© Copyright 2008 SystemExperts Corporation. All rights reserved.

## ▶ Payment Card Industry Data Security Standard

### The Skinny

Let us just jump right to the bottom line. The Payment Card Industry (PCI) has decided that organizations that transmit, store, or process credit card data, in particular, the Primary Account Number (PAN), must be compliant with the PCI Data Security Standard (DSS). Once you start using payment card data, the compliance is mandatory, all encompassing, and immediate.

### Understanding PCI-DSS a Little More

The PCI-DSS states that “PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply”. Thus if you use the PAN in any manner, you are required to be in compliance with the PCI-DSS. Further, if you fall under PCI-DSS, there are other classes/types of data handling requirements. These are shown in the table below.

The mandate for PCI-DSS compliance has been agreed to by the following card brands: Visa, MasterCard, American Express, JCB International, and Discover Financial Services. Another little item is that there are other protection requirements for ancillary data in the PCI-DSS. The PCI-DSS 1.1 standard can be found at the following URL: [www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](http://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf).

### Compliance

The current PCI-DSS standard specifies 12 requirements for compliance, organized into six logically related groups, which are called “control objectives.” They are defined as follows

#### Build and Maintain a Secure Network

- ▶ Requirement 1: Install and maintain a firewall configuration
- ▶ Requirement 2: Do not use vendor-supplied defaults

#### Protect Cardholder Data

- ▶ Requirement 3: Protect stored cardholder data
- ▶ Requirement 4: Encrypt transmission of cardholder data across 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

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name	YES	YES	NO
	Service Code	YES	YES	NO
	Expiration Date	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

## ▶ Payment Card Industry Data Security Standard

### Regularly Monitor and Test Networks

- ▶ Requirement 10: Track and monitor all access to 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

Thus for any company that falls under PCI-DSS, they must be 100% compliant with the requirements in all Control Objectives. This is harder than it seems, as the 12 requirements are actually further broken down into 206 specific requirements (211 for Hosting Providers).

The two bright spots in the process are “compensating controls” and “cardholder data environment (CDE)”. By limiting the definition of the CDE, you limit what systems come under PCI-DSS, and by using “compensating controls” you can meet the “intent” of a requirement, even if you don’t meet the exact letter of it.

It is important to note that if a company is not compliant, its risk losing their ability to process credit card payments and it may also incur fines. It can’t be overstated that from our understanding compliance is *mandatory, all encompassing, immediate, and perpetual* regardless of how big or small or the type of user you are. Meaning you have to do it, it must be 100%, it starts as soon as you start using cardholder data, and it lasts until the last bit of cardholder data is no longer used. Many companies don’t seem to understand how deep and lasting the claws of PCI-DSS are.

### Assessments: Proving Compliance

PCI requires that anyone under the PCI-DSS prove their compliance via annual assessments. There are four different levels of assessments that can be performed. Which level an organization falls under is roughly determined by how many credit card transactions a company performs coupled with the total value of these transactions as well as the type of entity (e.g., all service providers must pass a Level 1 assessment). Each card brand, not surprisingly, has its own definition for each level: however, they have been merging over time. The table below summarizes the most common level requirements:

Level	Assessments
1	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
2	Annual Self-Assessment Questionnaire and Quarterly Network Scans
3	Annual Self-Assessment Questionnaire and Quarterly Network Scans
4	Annual Self-Assessment Questionnaire and Annual Network Scans

## ▶ Payment Card Industry Data Security Standard

---

The three different types of assessments: Annual Onsite PCI Data Security Assessment, Annual Self-Assessment, and the Network Scans carry additional requirements for who can perform them:

- ▶ Annual Onsite PCI Data Security Assessment: PCI Qualified Security Assessor (QSA)
- ▶ Annual Self-Assessment Questionnaire: In-house staff
- ▶ Network Scans: PCI Approved Scanning Vendor (ASV)

It should be noted that many organizations that are required to perform the Annual Self-Assessment Questionnaire often use a third party consulting firm that specializes in these kinds of assessments to help them perform the audit to ensure completeness<sup>1</sup>. Failure to pass an assessment may result in having a company's ability to accept the credit card(s) revoked.

### A bit more on QSAs

To become a Qualified Security Assessor Company (QSAC) and a Qualified Security Assessor (QSA) there are three things that a company and the staff members who are looking to become QSA certified must do. First, the company must submit an application — which includes business licenses, substantial experience in the security uses, insurance certificates, registration fee, and other required documents — which will be reviewed by the PCI Council. If accepted, the company will be notified and invited to schedule training for its employees.

Second, the individuals from that company that will perform the assessments must attend a sanctioned QSA training course. They will be informed after the exams whether or not they passed or failed and whether they have qualified to be a QSA.

Third, after the Council has received the enrollment fee, the company will receive a Letter of Acceptance from the Council and each staff member who has passed will also receive a Certificate of Qualification. At that point the company and the staff members who passed the test will be listed in the Council's database of certified personnel. The following link can be used to look for certified QSAs: [www.pcisecuritystandards.org/qa\\_lookup](http://www.pcisecuritystandards.org/qa_lookup)<sup>2</sup>.

The process to become and maintain the QSA certification is significant, and arguably one of the most stringent in the security industry. PCI Security Standards Council is doing its best to ensure that organizations and people doing the assessment work are qualified and able to deliver a quality product.

### The Last Word

Any company that stores, transmits, or processes credit cards for Visa, MasterCard, American Express, JCB International, and Discover Financial Services must perform an audit against the PCI DSS. Compliance to the security requirements is mandatory, encompassing, and immediate.

The type of assessment and the determination of who can perform this assessment depend on how the organization is classified by each card brand. Level 1 assessments are the most rigorous and formal and must be performed by certified QSAs. Other assessments, depending on how the organization is classified, can be performed by the merchant themselves, or some one else on their behalf, whether they are a QSA or not.

---

<sup>1</sup> If a company has a breach and is found to have been out of compliance at the time of the breach, it will be held responsible. The mere fact that it completed an assessment does not protect the company in any way. The point of the PCI assessments, unlike many other standards assessments is not a "check box", but to ensure that a company IS DOING what they should be.

<sup>2</sup> Unfortunately, this interface does not allow for wildcards and one must supply at least a Last Name or Certificate ID as well as the Company name (e.g., one cannot just enter in a last name if you are not sure of the company nor can you enter in the company to see all qualified QSAs within a particular company).