

## **PCI Compliance: Frequently Asked Questions**

**By Andrew Plato, CISSP, CISM, QSA**  
**President / Principal Consultant**  
**Anitian Enterprise Security**

PCI compliance is on the minds of a lot of IT people these days. And, as usual, the forces of FUD (fear, uncertainty & doubt) are hard at work trying to confuse you. This article answers some basic questions about PCI and the Data Security Standard.

### **What is PCI?**

PCI stands for Payment Card Industry. The main standard established by the PCI Security Standards Council is the Data Security Standard or “DSS”. The standard consists of twelve requirements as defined below:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder 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

These requirements are pretty straightforward. They mandate some basic security controls and practices for an environment. Essentially, if you have a reasonably mature security program within your organization, PCI compliance is not difficult to achieve. If you do not have a mature program, then obtaining PCI compliance is a good opportunity to build one.

### **Merchant Levels**

There are additional implementation requirements depending on the annual number of credit card transactions processed by the merchants, which are broken down into levels. Each of the payment brands defines their own “levels” for merchants. The Visa merchant levels are the most common ones used to define a level:

- Level 1: Merchants processing more than 6,000,000 transactions per year or merchants who have already experienced a breach. Also, any company that is considered a “gateway” that is does processing for other companies / subsidiaries.
- Level 2: Merchants processing 1,000,000 to 6,000,000 transactions per year.
- Level 3: Merchants processing 20,000 to 1,000,000 transactions per year.
- Level 4: Any merchant processing fewer than 20,000 transactions per year.

Its actually harder than most people realize to be a Level 1 merchant . Six million transactions per year works out to about 17,000 transactions per day, every day. Merchant levels are very important because they are used to define expectations and standards. The requirements for Level 1 merchants are more stringent then the lower levels, as discussed further below.

**Does PCI apply to our company?**

Does our firm accept, process, store or transmit ANY credit card data on computer systems and/or a network? If your answer is yes, then PCI applies to your company. Naturally, if you do not store credit card data, then only parts of PCI would apply. Nevertheless, any form of transactions does require compliance.

**We use a third party firm to process our transactions, does PCI apply to us?**

Yes, it probably does. If you do any kind of credit card processing over a network (either internal or external) then PCI applies to your organization. Even though your firm may not store the credit card numbers or data, you still accept them and transmit them to your provider. As such, parts of the PCI standard will apply to your business. Moreover, your card processor will likely require you to be PCI compliant and may impose penalties or discontinue your service if you are not compliant.

**How many firms pass the first assessment**

To date, no company in the United States has passed their first assessment. About 80% of the Level 1 merchants are considered compliant as of Q3-2008. It is estimated that only about 20% of level 2-4 merchants are PCI compliant.

**What are the deadlines for compliance**

Level 1 Merchants were required to be compliant as of September 30, 2007. Level 2 merchants are required to be compliant by December 30, 2007. There is some debate if there will be any leniency on those deadlines.

**What are the penalties?**

Each of the payment brands has their own penalties. Visa tends to set the standard here as well:

- Fines, up to \$25,000 per month for being out of compliance.
- Increase in transaction fees.
- Suspension of credit processing privileges.

Visa and other payment cards have already levied fines on some merchants for failure to meet PCI requirements.

**How do we become compliant?**

An assessment is a good place to start. The PCI Standards Council publishes a list of Qualified Security Assessors Companies (QSAC). These are firms that are trained in performing PCI assessments. It is best to hire a QSAC since they have the training and experience to conduct PCI assessments and are best suited to provide you insight into the PCI compliance process.

The key to PCI compliance can be summarized in the following steps:

1. Get Executive Buy In: Management must be on board to become compliant, and you must have the resources (both time and money) to work on compliance.

2. **Assessment:** Get a security assessment to determine your security posture. Locate a QSAC that can perform an assessment for you. (Anitian is a QSAC.)
3. **Coordinated Planning:** Based on your assessment results, plan your remediation efforts in a coordinated manner with the expert help of a skilled security analyst who understands best practices for PCI remediation.
4. **Implement Policies and Controls:** Once you have determined all the controls and improvements necessary, implement them as needed. It is best to start on the outside with perimeter security improvements and move inward to applications and databases.
5. **Document, Document and Document:** One of the most important components of PCI compliance is having detailed documentation of internal processes and procedures, and can demonstrate they are being followed.
6. **Conduct Regular Scans and Tests:** You should conduct quarterly external tests and yearly security assessment tests of both internal and external systems.

**Our IT vendor offers a “PCI Compliant Product”, Will that take care of our compliance?**

No. PCI compliance is not an appliance you purchase nor is there any such thing as a “PCI compliant” product. PCI-DSS compliance is a process, not a product. Beware of desperate resellers and vendors selling anything that promises to make you PCI compliant.

**What does Anitian offer surrounding PCI?**

Anitian can offer a comprehensive remediation and assessment services surrounding PCI. Anitian has a team of Qualified Security Auditors and Anitian is a QSAC, approved to do PCI assessments. Contact your account executive to discuss how Anitian can help you.

**Where can I get more information?**

<https://www.pcisecuritystandards.org/about/faqs.htm>