

PCI Compliance Information - 2010

What is the PCI compliance standard?	1
Who must be compliant with the PCI standard?	2
Do organizations using third-party processors have to be PCI-compliant?.....	2
What are the PCI compliance deadlines?	2
Do all organizations have the same reporting and validation requirements for PCI compliance?	2
What are the PCI compliance "levels" and how are they determined?	3
What technologies are considered PCI-compliant?.....	4
Do companies need a PCI compliance assessment from a QSA?	4
What are the penalties for noncompliance?	4
What type of regular scanning/security testing is required for the PCI compliance standard?	4
What type of regular scanning/security testing is required for the PCI compliance standard?	5
What are the most common problems that companies experience with PCI compliance?	5

What is the PCI compliance standard?

The PCI Data Security Standard (PCI DSS) is a set of security and business requirements designed to ensure that companies that process, store or transmit credit card information maintain a secure environment.

The standard is administered by the PCI Security Standards Council, an independent body that was created by the main payment card brands (Visa, MasterCard, American Express, etc.). The council oversees the administration and management of the standard.

The payment brands are ultimately responsible for enforcing compliance -- not the government. PCI compliance is ultimately something that financial institutions, also called acquirers, must comply with. Those institutions pass on that compliance to their merchants and other organizations involved in credit card processing, storage and transmission.

Who must be compliant with the PCI standard?

Any company who "stores, transmits or processes" credit cards must be compliant with the PCI standard. This is a very broad definition and encompasses just about any company that accepts credit cards as a form of payment.

Do organizations using third-party processors have to be PCI-compliant?

Yes. Merely using a third-party company does not exclude a company from PCI compliance. It may cut down on their exposure and thereby reduce the scope of PCI efforts. However, it does not mean they can ignore PCI.

What are the PCI compliance deadlines?

Yesterday. All the major deadlines have already passed. All companies need to be compliant right now.

Do all organizations have the same reporting and validation requirements for PCI compliance?

Not exactly. The standard defines three different types of organizations that must be compliant: acquirers, merchants and service providers (these can be third-party providers, or TPPs, or gateways).

Acquirers are the banks or financial institutions that issue credit cards. Ultimately, it is the acquirers who are responsible for compliance of merchants and TPPs. Merchants are companies who accept cards for goods and services. TPPs are organizations that provide services for merchants that handle credit card information (such as an off-site storage facility.)

While the standard is the same for all organization types, the reporting and validation requirements are different for each. For example, gateways have a much stricter reporting and validation requirement than merchants, namely because they process cards from many merchants, not just one.

What are the PCI compliance "levels" and how are they determined?

Each organizations type has different level requirements. If a company is a gateway, for example, there is a good chance they are Level 1 and must have a Qualified Security Assessor (QSA). Merchants are a different story.

Service providers also have their own levels. Visa tends to set the standard here.

Service Provider Level	Description
1	All VisaNet Processors, OR All Gateways, OR All TPPs that handle Amex or Discover, OR All TPPs that handle more than 1M MasterCard accounts.
2	All Visa TPPs that handle more than 1M accounts per year, OR All Mastercard TPPs that handle less than 1M accounts per year.
3	All Visa TPPs that handle less than 1M accounts per year.

The merchant levels are the most commonly known. Each payment brand sets its own levels. Visa's levels tend to be the most restrictive and therefore are often used as the de facto level for merchants.

Merchant Level	Description
1	Any merchant -- regardless of acceptance channel -- processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant -- regardless of acceptance channel -- processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants -- regardless of acceptance channel -- processing up to 1M Visa transactions per year.

What technologies are considered PCI-compliant?

There is no such thing as a PCI-compliant product. The PCI standard does not certify products. Some products will help with PCI compliance, but there is no single product or group of products that will ensure complete PCI compliance. Beware of companies that say things like, "You must use our product to be PCI-compliant." This is an outright lie.

Do companies need a PCI compliance assessment from a QSA?

No. Only Level 1 merchants, gateways and service providers are required to have an annual assessment from a QSA. Level 2-4 merchants can choose to self-certify. However, self-certification carries some risks. If a self-certified company experiences a breach, they could, at the sole discretion of their acquiring bank, be required to have a Level 1 assessment every year.

It is beneficial to engage the services of a QSA since they have had training on the standard and tend to know it very well. The training for QSAs includes a lot of details on how to interpret the standard. Without that training, the PCI compliance standard can be easily misinterpreted.

What are the penalties for noncompliance?

The payment brands may, at their discretion, fine an acquiring bank \$10,000 to \$100,000 per month for PCI compliance violations. The banks will most likely pass this fine on to the merchant, gateway or service provider. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be brutal and decisive if levied. But penalties are really just the tip of the iceberg. Civil litigation from credit card holders and/or other institutions could quickly bankrupt a company.

What type of regular scanning/security testing is required for the PCI compliance standard?

As with many things, it depends on many factors. However, the actual assessment part is not the most expensive part. Remediation work is what can be very expensive. Smaller companies should plan for spending at least \$10,000 to \$25,000 on compliance. Larger firms have been known to spend as much as \$3 million to \$5 million on PCI compliance. The more problems you have, the more expensive it will be.

What type of regular scanning/security testing is required for the PCI compliance standard?

The PCI compliance standard requires that all merchants have quarterly external scans performed. These must be performed by an Approved Scanning Vendor (ASV). Only levels 1-3 are required to have quarterly scans. It is, however, recommended for level 4s. ASVs must be approved by the PCI standards council.

Additionally, the standard does require that firms have a yearly penetration test. This is different from scanning. Scans merely look for known exploits and weaknesses. A penetration test attempts to actually break into the network and gain access to resources. A penetration test is much more involved. Companies are not required to outsource this function, but realistically they should, since it would be difficult to prove that good penetration testing skills exist in-house.

What are the most common problems that companies experience with PCI compliance?

The two most frequent problems with PCI compliance are inadequate policies and improper network segmentation.

Organizational security policies must specifically address the components of the PCI standard. Many companies either outright lack policies or do not have them mapped to the standard. It's an easy thing to overlook, but it is required by the standard.

The more common and problematic issue is network segmentation. It is very important for companies to separate their payment systems from the rest of the network. This dramatically decreases what needs to be considered PCI-compliant. If payment systems reside in the same network as a print server or domain controller, then all those systems must meet the same PCI standards. If payment systems are isolated into a separate, secured network, then a company can decrease their exposure and limit what is "in scope" for a PCI assessment.
