



Article published on February 28th 2012 | [Business](#)

Many merchants might not realize that an integral part of maintaining required PCI compliance services involves using PCI compliant hosting as well. Not carrying over the standards of compliance to the hosting services can cause problems down the road.

## >> What Are PCI Compliance Services?

The major credit card issuers created consistent standards to be used within the payment card industry, or PCI. This is done to ensure high levels of security during transactions and protect personal information in the process. Every player on the PCI team – banks and other financial institutions, credit card companies, and merchants alike – are all bound by these guidelines if they want to accept credit cards. Disregarding these requirements is met with sanctions ranging in severity from fines to losing the ability to process cards altogether.

## >> The Elements of Compliance

There are six basic categories that are addressed when outlining PCI compliance services standards:

- \* Network security
- \* Data Protection
- \* Threat management
- \* Strict access control
- \* Regular testing and monitoring
- \* Specific company security policies

Each one of these six areas is further subdivided to address the specifics of achieving the parent goals; in all, there are twelve total PCI requirements.

## >> The Role of PCI Compliant Hosting

The above list makes it easier to see how vital it is to ensure that the hosting services are PCI compliant. Something as simple and common as a shared hosting plan may indeed render a company non-compliant. To make things more complicated, sometimes hosting providers are themselves not sure exactly what steps they need to take to meet the stringent guidelines.

## >> PCI Compliant Hosting: What to Look For

There are some specific essentials that are critical to providing adequate protection.

- \* Database protection: There should be a hardware firewall between servers on the Web and database; the database server has to be protected by a firewall.
- \* Separate servers: The database that houses credit card information must be on a separate server

from the site itself.

\* IP range: The database server has to be on a private IP range.

\* Monitoring the system: Files should be scanned for integrity, and hosts need to scan them on their level as well. Logs should also be reviewed for abnormalities at least daily.

\* If requested, the provider must be able to provide documentation to prove compliance with PCI policies.

>> Be Your Own Advocate

Finally, don't assume that hosting providers know the specifics of PCI compliance services. Do the homework and go in prepared with a list of questions to ask, both for your own protection and the protection of your business. The Web server is one of the most obviously vulnerable points in an online business, and failing to give it the proper protection by verifying PCI compliant hosting yourself puts you at risk of hacking, fines from PCI and possibly the inability to conduct business via credit card going forward.

Article Source:

<http://www.articleside.com/business-articles/pci-compliant-hosting-essential-part-of-compliance-services.htm> - [Article Side](#)

[Alex Taylor](#) - About Author:

At PCI Hosting, Get all kind of hosting services which includes reseller hosting, hosting provider services, a [pci compliant hosting](#), hipaa compliant web hosting and dedicated web hosting.

Article Keywords:

pci compliance services, pci compliant hosting

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!