

PCI: Protecting Cardholder Data

How it's changing the way YOU do business!

PCI Compliance is not a one-time event, it's a continuous process. Pursuant to PCI DSS, you must validate your compliance once a year.

There are three ongoing steps for validating PCI DSS:

1. **Assess:** Identifying cardholder data, taking inventory of your IT assets and business card processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.
2. **Remediate:** Fixing vulnerabilities and only storing cardholders data when you really need it.
3. **Report:** Compiling and submitting required remediation validation records (if applicable), and submitting compliance reports to the acquiring bank you do business with.

Use the following checklist to help you prepare for PCI Compliance over the next two years.

Suggested 2009 Activities:

- Register with Trustwave or another certified QSA.
- Become educated about PCI. There are many websites that provide this information.
- Determine if you will complete the self assessment form yourself (available at www.pcisecuritystandards.com) or if you will pay a nominal fee and hire an auditing company to help you through the process.
- Identify where key investment will be required (hardware, operations, etc.)
Updates are due by July 7, 2010.
- Complete the Self Assessment Questionnaire by December 2009 and identify any gaps for remediation.
- Begin remediation work.

Suggested 2010 Activities:

- Continue PCI educations/awareness.
- Begin remediation work.
- Complete any remediation activities required from 2009 assessment.
- Validate yourself as PCI DSS Compliant.