



Apple MacBook  Authorized Reseller  With Intel Core 2 Duo and Front Row \$1099 [Learn More](#)

# Biztech

 [GO](#)  BizTech

[BizTech](#) » [What's New](#) » [Best Practices: PCI Compliance](#)

[ [What's New](#) ]

» [comment](#)

» [print](#)

» [email](#)

## Best Practices: PCI Compliance

### 10 Steps for Securing Credit Card Data

By Jeremy Simon



Mandated since June 2001, the Payment Card Industry Data Security Standard (PCI DSS) specifies a broad range of technical, administrative and physical security controls for protecting credit card data. While the PCI DSS is made up of only 12 main requirements, they are divided into more than 200 subrequirements, all of which must be satisfied in order to be considered fully compliant.

The PCI DSS provides a well-defined list of security requirements, but many organizations are left with more questions than answers when it comes to determining how best to address each requirement in a manner that will be considered acceptable for PCI compliance.

When approaching PCI compliance, much of the effort can often be handled in-house, but it's also important to know when to ask for help. Misinterpretation of PCI requirements can lead to costly mistakes. To address the need for expert guidance, the PCI Security Standards Council maintains a program for training Qualified Security Assessors (QSAs). A QSA is not intended to be merely an auditor but is also meant to act as an advisor to organizations working to achieve PCI compliance. QSAs are trained to provide clarification of the underlying intent of the PCI requirements and to assist organizations in identifying reasonable means of obligations.

The following step-by-step approach for becoming PCI compliant will help the organization avoid many of the pitfalls associated with the process:

#### 1. Educate Yourself.

Read the PCI DSS, preferably several times. Ensure you understand

#### RELATED

**Best Practices for**  
10 steps to ensure smoother.

**Moonlighting 101**  
Blogging is all the employees blog, or legal ramifications.

**Protecting Your IT**  
Avoid the journey of by exiting at the encrypted drives.

**Should IT Have an Oath?**

Medicine has the heavily regulated and licenses its practitioners restricts the prescription what about IT?

**Restricted Airspace**  
Protect your wireless latest generation of

**Avoiding Legal Liability**  
It takes more than encryption to safeguard want to keep legal bay.

**Protective Order**  
Thomas Salzman : Esq., provide legal

**Lexar ExpressCard 16GB**

Performance storage and backup.

**\$249.99**

Learn More >

crucial TECHNOLOGY

CDW

requirement and try to see the underlying intent of each. In questions you have. Read PCI-related forums and blogs to see what companies are addressing PCI compliance issues. It's often a QSA at this point, to provide direction and answers to questions that inevitably arise during the process of becoming PCI compliant.

## 2. Determine Your PCI Classification.

Work with your acquiring bank to determine what Merchant Provider classification level applies to your organization for validation purposes. Each acquiring bank is responsible for the compliance of all of its merchants, so the bank has the authority to determine your company's PCI classification level. A QSA can help you determine your classification will likely be assigned based upon acceptance of transaction volume, but in the end, the bank has the final say.

## 3. Perform Data Discovery.

Find out where cardholder data currently exists in your environment. Identify all payment acceptance channels, and map cardholder data across the network, and identify all places where that data is stored. It is helpful to create a network diagram that shows network segments where key systems reside — then map the cardholder data flow onto this visual representation of where credit card data is transmitted, processed or stored in your network.

## 4. Whenever Possible, Eliminate Cardholder Data Instead of Securing It.

Securely dispose of any cardholder data that is not required. This might help to reduce the scope for PCI compliance and reduce the costs associated with becoming compliant. Most companies will still need to retain credit card data but it's stored in a centralized, tightly controlled manner. Some organizations that handle only a small volume of transactions that it's easier and less expensive to completely outsource all credit card processing to a third party. If this approach meets compliance requirements might no longer apply at all (check with your banking institution to be sure).

## 5. Define the Scope for PCI Compliance.

Now that you know where the cardholder data exists, who has access to it, and how the network is segmented, PCI compliance can be determined. The entire enterprise (in terms of both network and staff) might not necessarily be within the scope of PCI compliance — and proper scoping is essential to controlling costs for PCI compliance. Test to all systems that store, process or transmit cardholder data, as well as any systems connected to those (in other words, systems on the same network segment, not separated by a firewall). Because scope is such a critical aspect of PCI compliance is a good point to confirm your scoping approach with a QSA to ensure it will be considered acceptable by PCI auditors.

## 6. Perform a Gap Assessment.

Perform a gap assessment based upon the established PCI scope. Determine whether each requirement is satisfied by your systems. The PCI Audit Procedures provide additional details regarding how to validate the presence of each requirement. Every single requirement must be addressed for full compliance — but compensating controls are allowed, as long as the criteria are met (see [PCI DSS, Appendix B](#)).

## 7. Implement Changes to Address Noncompliant Findings.

Build a remediation plan to address noncompliant findings. Implement required controls, write policies, update procedures. This step can often turn into an extensive process, depending on the present state of information security and governance of your organization. PCI requirements include technical, physical and administrative controls, so organizations without an information security program will find there's a lot to be built in order to address PCI requirements. This is another point where

work with a QSA. A good QSA should be able to help you come up with a cost-effective remediation strategy that works for your particular business.

### 8. Perform Quarterly Vulnerability Scanning and Annual Penetration Testing.

Find an authorized scan vendor (see URL below) to scan all Internet accessible systems on a quarterly basis. Rescan until a fully compliant scan report is obtained. In addition to quarterly vulnerability scanning, organizations must also perform penetration testing (network and application layers) at least annually or when significant changes are made to the environment.

### 9. Provide Validation of PCI Compliance.

Have an onsite audit performed, or complete the self-assessment questionnaire. Submit the Report on Compliance Assessment Questionnaire, along with the quarterly scan results, to your acquiring bank (for merchants) or to Visa or Mastercard providers).

### 10. Stay Compliant Through Ongoing Security Maintenance.

Maintain security controls according to guidelines outlined in the PCI DSS to ensure ongoing compliance. There is a special protection for organizations that can demonstrate they were in full compliance with the PCI DSS *at the time of a breach*. It's important to not only *become* compliant but also *stay* compliant.

The following are additional reference materials that are available online and may be useful:

- [pcisecuritystandards.org](http://pcisecuritystandards.org) — The official PCI Council Web site, where you can find all of the official documents. You'll want to download and read at least the following:
  - Self-Assessment Questionnaire  
[pcisecuritystandards.org/pdfs/pci\\_saq\\_v1-0.pdf](http://pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf)
- Visa Cardholder Information Security Program overview  
[usa.visa.com/download/merchants/cisp\\_overview.pdf](http://usa.visa.com/download/merchants/cisp_overview.pdf)

---

*For the last 10 years, Jeremy Simon, PCI QSA, CISSP, CISA, has served as partner and CTO of Hallock Security (www.hallock.com). With more than 15 years of experience in information security consulting, Simon's primary focus over the last years has been providing PCI compliance advisory services, and he has worked with companies of all types in achieving PCI compliance.*

---

### [ Related Articles ]

- [Best Practices for PCI Compliance](#)
- [Moonlighting 101](#)
- [Protecting Your Loved Ones](#)
- [Should IT Have Its Own Hippocratic Oath?](#)
- [Restricted Airspace](#)
- [Avoiding Legal Landmines](#)
- [Protective Order](#)