Compliments of QUALYS®

PCI Compliance FOR DUMMIES®

Qualys Limited Edition

Secure and protect cardholder data

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Sumedh Thakar
Terry Ramos

PCI Compliance FOR DUMMIES®

by Sumedh Thakar and
Terry Ramos

WILEY
A John Wiley and Sons, Ltd, Publication

PCI Compliance For Dummies®

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

Email (for orders and customer service enquires):
cs-books@wiley.co.uk

Visit our Home Page on www.wiley.com

Copyright © 2009 by John Wiley & Sons Ltd, Chichester, West Sussex, England

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London, W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, or emailed to permreq@wiley.com, or faxed to (44) 1243 770620.

Trademarks: Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER, THE AUTHOR, AND ANYONE ELSE INVOLVED IN PREPARING THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-0-470-74452-9

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Introduction

Welcome to *PCI Compliance For Dummies*! Compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) is mandatory if your company stores, processes, or transmits payment cardholder data. This book is all about understanding PCI and how merchants can comply with its requirements.

About This Book

This book simply explains the PCI Data Security Standard and describes its requirements for compliance. After reading this book you'll know more about how to comply with the PCI Data Security Standard.

Foolish Assumptions

In writing this book, we assume that you:

- Are a merchant and know you have to comply with PCI but aren't sure what's required or what you need to do.
- Are familiar with information technology and networking.
- Want to discover the easiest, most effective and direct way to fulfill compliance requirements for PCI.

How to Use This Book

This book is divided into five succinct and easily-digestible parts:

- **Part I: Merchants: Cardholder Data Thieves Want You!** Start here if you need a primer on security risks faced by merchants who accept payment cards.
- **Part II: Looking at the Big Picture of PCI Standards.** Understand the three PCI standards and how each applies to merchants.

- **Part III: Surveying Requirements of the PCI Data Security Standard.** An introduction to the six goals and 12 requirements of PCI DSS.
- **Part IV: Verifying Compliance with PCI.** Become familiar with the tools and reporting requirements for compliance, and discover where merchants can go for help.
- **Part V: Ten Best Practices for PCI Compliance.** Follow this short list of steps to ensure compliance with the PCI standard.

Dip in and out of this book as you wish; go to any part that interests you immediately; or read it from cover to cover.

Icons Used in This Book

We highlight crucial text for you with the following icons:

This icon targets hints and shortcuts to help you get the best from PCI scanning solutions.

Memorize these pearls of wisdom – and remember how much better it is to read them here than to have your boss give a know-it-all lecture.

The bomb means 'whoops'. It signals common errors that can happen. Avoid these at all cost.

Prepare for a little bit of brain-strain when you see this icon. But don't worry – you don't have to be a security whiz or hot rod programmer to do vulnerability scans required for PCI compliance.

Where to Go from Here

Check out the section headings in this book and start reading wherever it makes sense. This book is written with a sequential logic, but if you want to jump to a specific topic you can start anywhere to extract good stuff. If you want a hands-on demo or trial version of QualysGuard – our featured PCI scanning and reporting solution – visit `www.qualys.com`.

Part I

Merchants: Cardholder Data Thieves Want You!

In This Part

- Identifying the vulnerability of merchants to a payment card data breach
- Understanding the risks and consequences of a breach
- Reviewing risk points of the payment card transaction processing flow
- Using PCI as a way to control risks and protect cardholder data

To some people, the idea of crime against merchants might be a gun-toting thug (*'Empty your cash register – NOW!'*), a shoplifter, or perhaps a wily embezzler. A modern, more lucrative, and easier-to-exploit target is sensitive data for payment card accounts of a merchant's customers. With these data, criminals can unlock direct access to money and personal identities. Cyber thieves can easily send these data to distant cohorts for exploitation beyond the practical reach of law enforcement. Damage can be swift and punish merchants as well as the customer. Fallout varies, but when customers lose trust, they usually take their business elsewhere.

Fortunately, there's a clear path of action for merchants that can help prevent compromise of payment card data. The Payment Card Industry Data Security Standard is the authorized program of goals and associated security controls and processes that keep payment card data safe from exploitation. The standard is often called by its acronym PCI DSS. We simply call it PCI. This book, *PCI Compliance For Dummies*, can help merchants to quickly understand PCI, and how your organisation can use it as a tool to prevent breaches of cardholder data.

Compliance with PCI is mandatory for any merchant or other organization that accepts payment cards.

Merchants Have What Data Thieves Want

Personal consumer information has been under siege for years. Since January 2005, more than 245 million database records containing sensitive personal information have been involved in security breaches in the US alone, according to PrivacyRights.org.

The object of desire for data thieves is cardholder data – the primary account number (PAN) and sensitive authentication data printed on or stored in a magnetic stripe or chip on the credit or debit card. Cardholder data is the only information standing between thieves and your money. No wonder criminals seek it with intensity!

New research indicates the most vulnerable sector for data breaches is merchants. Merchants process the bulk of credit and debit cards offered for payment of goods and services. Smaller merchants are the most attractive targets for data thieves because they're less likely to have locked down payment card data. According to Visa Inc, more than 80 per cent of attacks on payment card systems target 'Level 4 Merchants' – those who process less than 1 million payment card transactions each year.

More than 6 million Level 4 Merchants operate in the US, processing about 32 per cent of all Visa transactions. Merchants who received most of the attacks included restaurants, traditional retailers with physical stores, and higher education institutions.

Overall, the number of attacks on payment card processing systems is rising. The number of attacks doubled from 2006 to 2007, a trend that appears to be continuing.

Cardholder data is the main target

In a Gartner survey of 4,500 consumers who experienced payment card fraud, about a third said they were unsure where the theft occurred. A data breach at a retailer or other third party was the largest category for known points of cardholder data theft (shown in Figure 1-1).

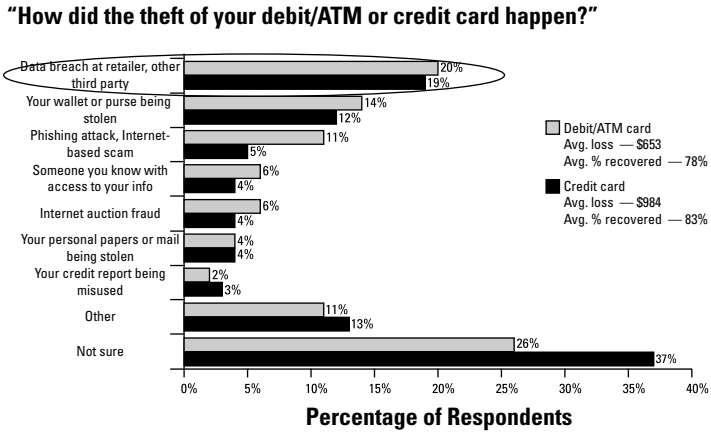


Figure 1-1: Consumers say breaches are the leading cause of card fraud. (Source: Gartner, Inc., May 2008)

Breaches can hit merchants of any size

Payment card data theft has hit organizations of all sizes. The biggest known breach to date was the theft and sale of more than 40 million credit and debit card numbers from nine major US retailers, including TJX Companies Inc., BJ's Wholesale Club Inc., OfficeMax Inc., Barnes and Noble Inc., and Sports Authority. The criminals were an international credit fraud ring and prosecution is now underway.

Cardholder data theft can also occur at small, 'mom and pop' stores. For example, in spring 2008, the ATM/credit card reader was switched in a small supermarket's checkout aisle in Los Gatos, California. At least 135 people were reported to have had cardholder data stolen via this rogue device. The small store is in a community in hi-tech Silicon Valley, so some victims could have included security technology experts! No one is immune.

Stories like these make consumers especially nervous about sharing cardholder data with online stores. Three quarters of Internet users are uncomfortable sending personal or credit card information over the Internet, according to Pew Internet. And aside from the huge roster of documented breaches, there's other evidence for concern. According to a study by the University of Michigan, 76 per cent of websites from 214 US financial institutions suffer from at least one security design flaw that prevents secure usage (you can find the full report at `http://cups.cs.cmu.edu/soups/2008/proceedings/p117Falk.pdf`).

Understanding the Potential Fallout from a Breach

Thanks to federal law and standard practice by the financial industry, the maximum cash exposure of a consumer whose cardholder data is stolen is just $50; the rest of all related losses are paid by the card companies. If the data allows a criminal to access other accounts or steal a consumer's identity, financial fallout could be severe for that individual. Resolving just one incident of a stolen identity may take years of effort. Personal fallout would be catastrophic if multiple breaches at different merchants occurred during a short period of time.

Merchants face their own types of fallout. When a breach occurs, there are discovery and containment costs for investigating the incident, remediation expenses, and attorney and legal fees. But this is just for starters. Long-term fallout for all merchants may include:

- Loss of customer confidence.
- Lost sales and revenue.
- Lower use of online stores due to fear of breaches.
- Brand degradation or drop in public stock value.
- Employee turnover.
- Fines and penalties for non-compliance with PCI and other regulations.
- Higher costs for PCI assessments when merchants with a breach must subsequently comply with the penalty of more stringent requirements.
- Termination of the ability to accept payment cards.
- Fraud losses.
- Cost of reissuing new payment cards.
- Dispute resolution costs.
- Cost of legal settlements or judgments.

The potential fallout for larger merchants can be huge, but isn't insurmountable if a company is well capitalized. Discount retailer TJX says it's spent $202 million in expenses related to the big data heist mentioned in the previous section – and it's just one of the nine large merchants affected by that breach.

Smaller merchants, however, may have significant trouble weathering a cardholder data breach. Think about your company's cash flow and whether it could cover potential damage from a breach. The risk of going out of business should be motivation enough to follow PCI and protect the data. But that's why you're reading this book, right? So let's get to work.

Exposing the Risks in Payment Card Processing

When a merchant accepts a payment card, a complex system of devices, software, networks, service providers and the card acquirer is required to process the payment and get the

money. Each element of the payment card technology system poses risks that could be exploited by criminals, so it's vital to use appropriate security controls and business procedures to minimize risk and protect cardholder data.

Obviously, a merchant can't control the entire payment card system. So PCI limits the scope of responsibility to protecting cardholder data with security technologies and processes that exclusively cover the merchant's domain, such as:

- Payment card readers used to swipe and collect data.
- Point of sale systems (including PCs and handheld devices).
- In-store and inter-store networks and devices (servers, wireless routers, modems, and so on.).
- Payment card data storage and transmission over the Internet to a merchant's distributed systems or service provider.
- Ensuring that third-party service providers, their applications and systems are compliant with PCI requirements.
- Access control to the card processing system.
- Network monitoring, scanning and vulnerability management.
- Company security policy.

Figure 1-2 illustrates domains under the merchant's responsibility – in this case, the POS and Merchant sections of the diagram and related network links.

PCI requirements can help your merchant organization implement the right controls and processes to avoid compromising cardholder data. The good news is that PCI doesn't request anything different from what you'd normally do security-wise to protect cardholder data. Part II introduces how PCI standards apply to merchants.

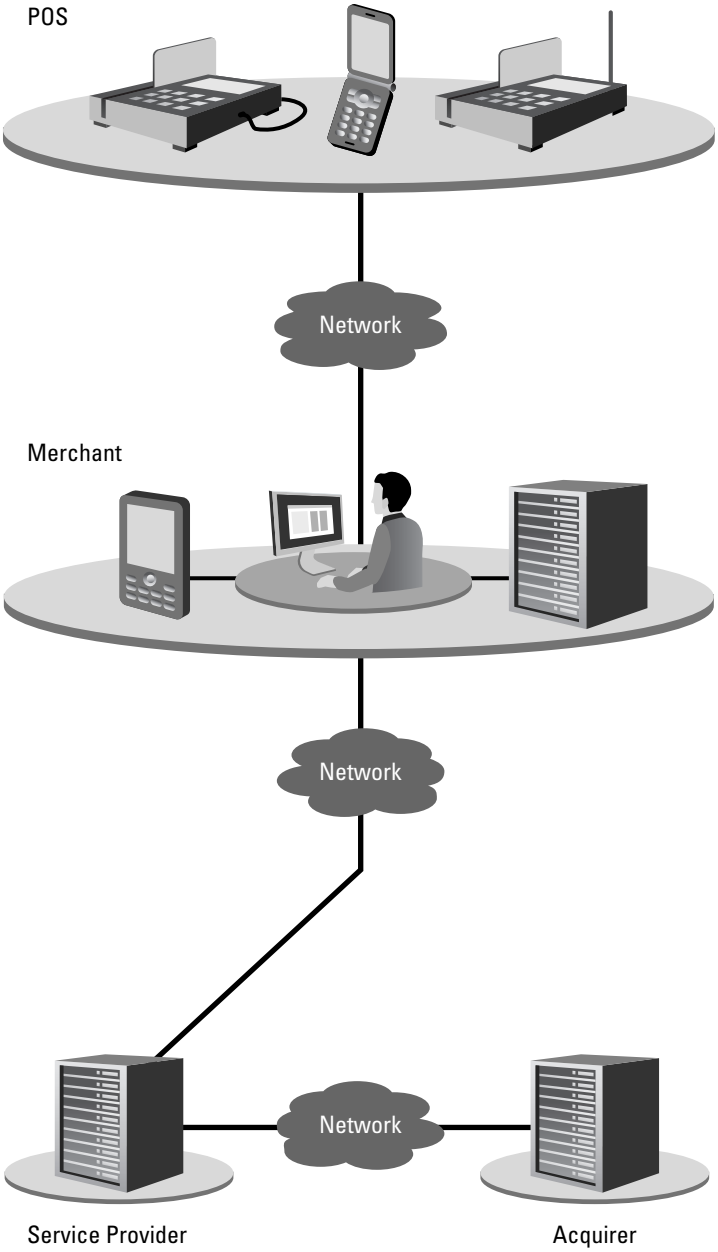


Figure 1-2: PCI requires merchants to protect systems under their control.

Risky business

PCI provides the guidelines to help merchants protect cardholder data. Unfortunately, merchants are a prime target for data thieves because they engage in activities that place cardholder data at risk. According to the National Federation of Independent Business (NFIB) Guide to Data Security:

- **37 per cent** of card-accepting businesses knowingly store customer card numbers.
- **24 per cent** store customer Social Security numbers.
- **28 per cent** store customer bank account numbers or copies of their checks.
- **52 per cent** of all small businesses keep at least one of these sensitive pieces of information.
- **57 per cent** don't see securing customer data as something that requires formal planning.
- **61 per cent** have never sought out information about how to properly handle and store customer information.

Part II

Looking at the Big Picture of PCI Standards

In This Part

- Understanding PCI and how its standards fit together
- Meeting PCI's manager, the PCI Security Standards Council
- Summarizing the PCI Security Standards

In this part we explore the three PCI standards. One is tailored for merchants and other organizations that accept payment cards; one for manufacturers of card devices used at the point of sale; and one for software developers of payment card applications. Each of these standards share the same primary goal: *protecting cardholder data*. Some cardholder data are printed on a card; others reside in digital format on a magnetic stripe or computer chip. Figure 2-1 shows the types of sensitive data and where they reside on a payment card.

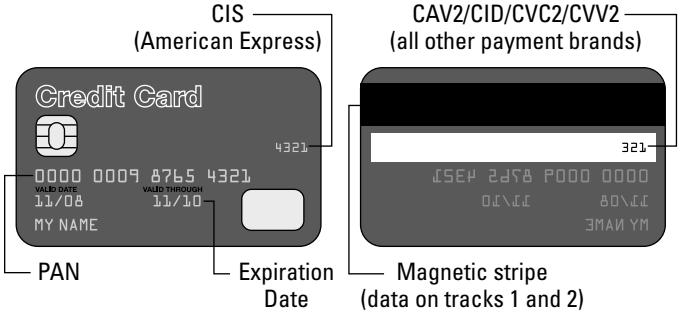


Figure 2-1: Types and locations of cardholder data on a payment card. (Source: PCI SSC)

Piecing the Puzzle: How PCI Standards Fit Together

PCI standards present technical and operational requirements for protecting cardholder data. The standards apply to any organization that stores, processes or transmits cardholder data. The PCI standards are tailored for three communities: merchants and processors, software developers, and manufacturers. They address the 'ecosystem' of retail payment devices, applications, card processing infrastructure, and the organizations that execute related operations.

Here's how the PCI standards relate to each other (see Figure 2-2):

- **PCI Data Security Standard** (PCI DSS) is the core standard, which is primarily for merchants and processors. It addresses security technology controls and processes for protecting cardholder data. This book is about PCI DSS, which we more simply call PCI.
- **Payment Application Data Security Standard** (PA DSS) is for software developers who sell commercial applications for accepting and processing payment cards. Most card brands require merchants and processors to use only approved payment applications.
- **PIN Entry Device Security Requirements** (PED) are for manufacturers of payment card devices used at the point of sale. In addition to other PCI DSS requirements, software developers, merchants and processors must use only approved devices compliant with PED.

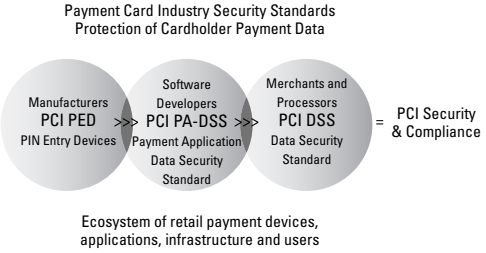


Figure 2-2: PCI is about protecting cardholder data. (Source: PCI SSC)

The Standards' Manager: PCI Security Standards Council

Every standard has its manager, and PCI is no different. An open global forum called the Payment Card Industry Security Standards Council (PCI SSC) develops, manages, educates, and raises awareness of the three PCI standards. The Council also provides documents to help merchants implement PCI (check out 'Getting Help: Council Resources for Merchants' at the end of this chapter).

The Council was founded in 2006 by the major card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Each brand recognized the importance of securing cardholder data, so they all agreed to incorporate the PCI Data Security Standard within their own compliance programs. The founders also recognize Qualified Security Assessors and Approved Scanning Vendors who are certified by the Council as resources for PCI compliance.

The five card brands share equal responsibility in Council governance, are equal contributors to the Council, and share responsibility for executing its work. The Council organization consists of an executive committee, a management committee, a general manager, marketing working group, legal, and technical working groups.

Other industry stakeholders participate in the PCI standards process. These include merchants, payment card issuing banks, processors, hardware and software developers, and other vendors. These stakeholders may review proposed changes to standards and vote on their official adoption by the Council.

The PCI Data Security Standard

The PCI Data Security Standard is the key standard for helping merchants to protect cardholder data. If your organization accepts just one card for payment, you must comply with PCI DSS. This standard describes the technical and operational system components that are part of or connected to cardholder data. PCI DSS is structured by six goals, that include 12

related requirements which we lay out in Table 2-1. The table is a handy overview – we go into the detail in Part III, and you can read about how to comply with PCI in Part IV.

Table 2-1 PCI Data Security Standard

Goals	*PCI DSS Requirements*
Build and maintain a secure network	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.
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	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.
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors.

Source: PCI SSC

The three important tools that play crucial roles with compliance are:

- **Card Brand Compliance Programs.** The major card brands have incorporated the PCI DSS into technical requirements for compliance. But each brand has variations in the process of verifying compliance so merchants need to check with their acquiring financial institution for specific requirements (see the nearby sidebar).
- **Qualified Assessors**. The PCI Security Standards Council qualifies two kinds of assessors to help merchants comply with PCI. The Qualified Security Assessor (QSA) is a consultant who assesses your organization's compliance with the standard. The Approved Scanning Vendor (ASV) validates compliance with the standard's external network scanning requirements. Some ASVs provide software or a web service to perform scans. Others will scan for you. See Part IV for details.
- **Self-Assessment Questionnaire**. Based on card brand requirements, some merchants are able to self-validate for compliance by completing a Self-Assessment Questionnaire (SAQ). Different kinds of SAQs suit different merchant operations. Part IV describes these and how to use the questionnaire, which is used primarily by Levels 2 to 4 merchants.

Delving deeper into card brand compliance programs

Want more information about card brand compliance programs? Check out:

- ***American Express:*** `www.americanexpress.com/datasecurity`
- ***Discover Financial Services:*** `www.discovernetwork.com/fraudsecurity/disc.html`
- ***JCB International:*** `www.jcb-global.com/english/pci/index.html`
- ***MasterCard Worldwide:*** `www.mastercard.com/sdp`
- ***Visa Inc.:*** `www.visa.com/cisp`

Revealing the PIN Entry Device (PED) Security Requirements

Cardholder data theft can easily start with insecure point-of-sale devices that accept personal identification number (PIN) entry for transactions. The PIN Entry Device Security Requirements (referred to as PED) were created to improve the security characteristics and management of these devices.

PED requirements apply to manufacturers of these point of sale devices. Manufacturers must provide a finished product for which physical and logical security is never compromised, either during the process of manufacturing or distribution to the merchant buyer.

Merchants are required to use only PIN entry devices that are approved by the PCI Security Standards Council. Before you purchase any PED, check the list of approved devices on the PCI Security Standards Council website. Merchant compliance with this point is checked every year. Here's a summary of the PED security requirements (source: PCI SSC):

- **Device Characteristics**
  - Physical Security Characteristics (to prevent the device from being stolen from its location).
  - Logical Security Characteristics (to provide functional capabilities that ensure the device is working).
- **Device Management**
  - Device Management during manufacturing.
  - Device Management between manufacturer and initial cryptographic key loading.
  - Considers how the PED is produced, controlled, transported, stored and used throughout its lifecycle (to prevent unauthorized modifications to its physical or logical security characteristics).

Payment Application (PA) Data Security Standard

Another place where thieves can attack is through payment applications used to store, process or transmit cardholder data during authorization or settlement. The Payment Application Data Security Standard (PA DSS) applies to creators of commercial off-the-shelf payment applications – and their integrators and service providers. If you use a custom payment application, PA DSS doesn't apply. Instead, you are responsible for making the application meet PCI DSS requirements.

The focus of PA DSS is preventing the compromise of full magnetic stripe data digitally stored on the back of a payment card. It also aims to protect cardholder data stored on the computer chip embedded on the front of some payment cards.

Most card brands encourage merchants to use payment applications that comply with PA DSS and are approved by the PCI Security Standards Council. Before you purchase a payment application, check the list of approved payment applications at `www.pcisecuritystandards.org`. Here's a summary of the Payment Application Data Security Standard requirements (source: PCI SSC):

- Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CIV2, CW2) or PIN block data.
- Provide secure password features.
- Protect stored cardholder data.
- Log application activity.
- Develop secure applications.
- Protect wireless transmissions.
- Test applications to address vulnerabilities.
- Facilitate secure network implementation.
- Do not store cardholder data on a server connected to the Internet.

- Facilitate secure remote software updates.
- Facilitate secure remote access to application.
- Encrypt sensitive traffic over public networks.
- Encrypt all non-console administrative access.
- Maintain instructional documentation and training programs for customers, resellers and integrators.

Is PCI the Law?

Is there a law that compels you to comply with PCI? One answer is: Sort of, but only in Minnesota.

In 2007, Minnesota passed the nattily named Minn. Stat. 365E.64, which prohibits storing data from the magnetic stripes on payment cards, plus related security codes and PINs for more than 48 hours after approval of a card transaction. This law is a subset of PCI, specifically related only to PCI DSS Requirement 3 ('Protect stored data'). Minnesota law also allows financial institutions to recover reasonable costs from a merchant related to the theft of cardholder data.

Legislators in at least 10 other states thought Minnesota's law was a good idea. Bills were introduced in Alabama, California, Illinois, Indiana, Iowa, Michigan, New Jersey, Texas, Washington, and Wisconsin. But none were passed.

During the past few years, proposals have also made rounds in the US Congress but none were passed.

When Governor Arnold Schwarzenegger vetoed California's bill, he said the payment card industry was in a better position to maintain the standard, and anything passed into law would end up conflicting with PCI DSS as the standard was revised. (This was after the state's Retailers Association and Chamber of Commerce lobbied that California's bill would drive up compliance costs.)

Other critics say that turning PCI into law would make the PCI Security Standards Council (and effectively, the card brands) a quasi-legislative, quasi-judicial body with the power to set regulations and punishments yet be accountable to no one.

Transforming PCI into law faces the same kind of challenges any good technology legislation would face. For example, after California passed a data breach notification law in 2002 (SB 1386), at least 40 other states passed

similar bills. Yet despite nearly universal requirements to disclose breaches to consumers, only four of the nine large retailers who recently suffered a breach of 40 million records clearly alerted their customers to the incident. Statutory enforcement of PCI requirements would be much more difficult.

For now, know that the full PCI Data Security Standard is not a law in any country or state. Instead, PCI is enforceable under private contractual conditions stipulated by each of the card brands. When a merchant accepts one card payment, it must abide by PCI and any side provisions decreed by that card's brand.

For more information about how to comply with PCI, head to Part IV of this book.

Getting Help: Council Resources for Merchants

The PCI Security Standards Council provides a variety of tools to help merchants understand the requirements of PCI DSS and the steps to verify compliance. You can find links to the following documents on the Council's website at `www.pcisecuritystandards.org`.

- Frequently Asked Questions (FAQ)
- Membership
- Webinars
- Training (for assessors)
- PCI SSC Approved PIN Entry Devices
- PCI SSC Approved Payment Applications
- The PCI Data Security Standard version 1.2 (PCI DSS)
- Navigating the PCI DSS
- Security audit procedures
- Glossary

- PCI SSC Approved Qualified Security Assessors
- PCI SSC Approved Scanning Vendors

Now that you have the big picture of PCI, turn to Part III and discover how to protect sensitive cardholder data with the detailed requirements for the PCI Data Security Standard.

Part III

Surveying Requirements of the PCI Data Security Standard

In This Part

- Gauging the effort for meeting PCI requirements
- Understanding where merchants should focus on security
- Comparing the two kinds of PCI requirements: technology and process
- Surveying the goals and requirements of the PCI Data Security Standard
- Reviewing the role of compensating controls for PCI requirements

As you go through this book, you may wonder how much of the information really applies to your business. The answer depends on the nature of your business operations, the volume of payment card transactions, and the complexity of IT resources that underpin your card processing infrastructure. If your business is a regional or national chain of stores, fulfilling PCI requirements will require more effort than smaller stores who don't have as much hardware and software to protect and whose business processes are usually simple. A single small mom-and-pop store will require the least effort to comply with PCI.

The great thing about PCI requirements is that they provide an excellent checklist for protecting cardholder data. The PCI Data Security Standard requirements are the same points you'd normally use for overall information and network security. By implementing security for PCI, you'll effectively use

the industry's best practices for security. And PCI not only will help you secure cardholder data – it also may fulfill security requirements for other laws and business regulations affecting your company. PCI is good for cardholder data security and good for your business.

Focusing on Security in the Payment Card Process

The payment card process is a system whose various components are each exposed to security risks. As shown in Figure 3-1, the front-line interaction is between cardholders and merchants. The merchants interact with a back-end system comprised of their own 'acquirer' (the merchant bank servicing a business), any of five payment card brand networks, and the card issuers.

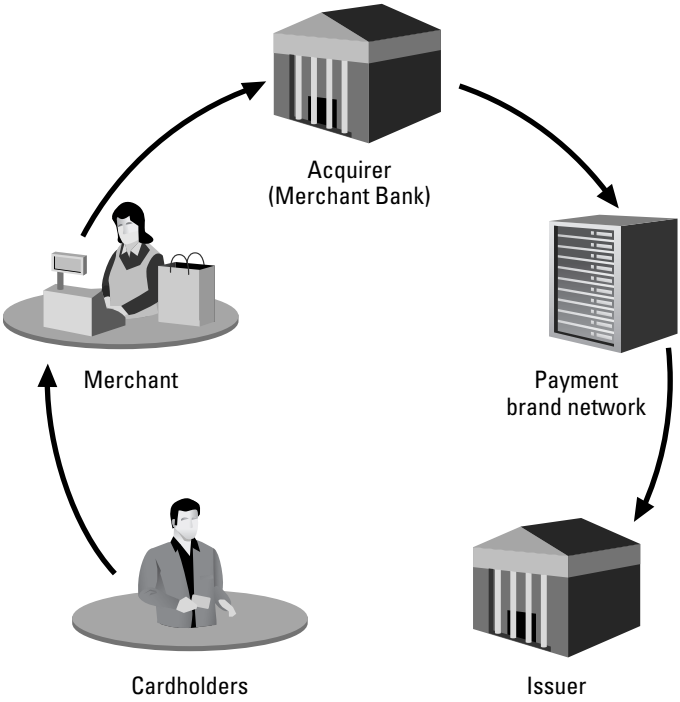


Figure 3-1: Card payment system.

The three steps to process a payment card transaction are:

- **1: Authorization.** The merchant requests and receives authorization from the card issuer, which enables the merchant to complete the purchase with the expectation of getting paid.
- **2: Clearing.** The acquirer and the issuer exchange information about the purchase via a network owned and operated by a payment brand.
- **3: Settlement.** The merchant's bank pays the merchant for the cardholder purchase and the cardholder's bank bills the cardholder or debits the cardholder account.

Obviously, merchants aren't required to handle security for all three steps. Merchants are expected to check with their third-party service providers and get their certificate of PCI compliance. Otherwise, the domain of a merchant's responsibility for PCI security is in the authorization phase of card processing (see Figure 3-2).

The authorization phase has many points of vulnerability that could expose cardholder data to unauthorized access. Merchants must secure cardholder data passing through several system elements, including:

- Point-of-sale PIN entry devices.
- Point-of-sale terminals.
- Servers used to process and store cardholder data.
- Payment applications.
- Internal networks used for cardholder data.
- Wireless access points.
- Routers, gateways and other network devices.
- Network connectivity with third-party card service providers and web-based shopping carts.
- Storage and backup systems used for cardholder data.
- Network-attached printers used for transferring cardholder data to paper.
- Paper-based storage systems.

- Portable devices that could link to cardholder data (laptops, handheld devices, USB-attached storage devices and smart phones for example).
- Insecure internal card processing procedures and access controls.
- Disgruntled employees or contractors.
- Guests with access to network with cardholder data.
- Poor physical security of the building and devices used for cardholder data.
- Poor procedures for monitoring security, finding vulnerabilities and fixing them.
- Lack of a policy or interest in security by management.

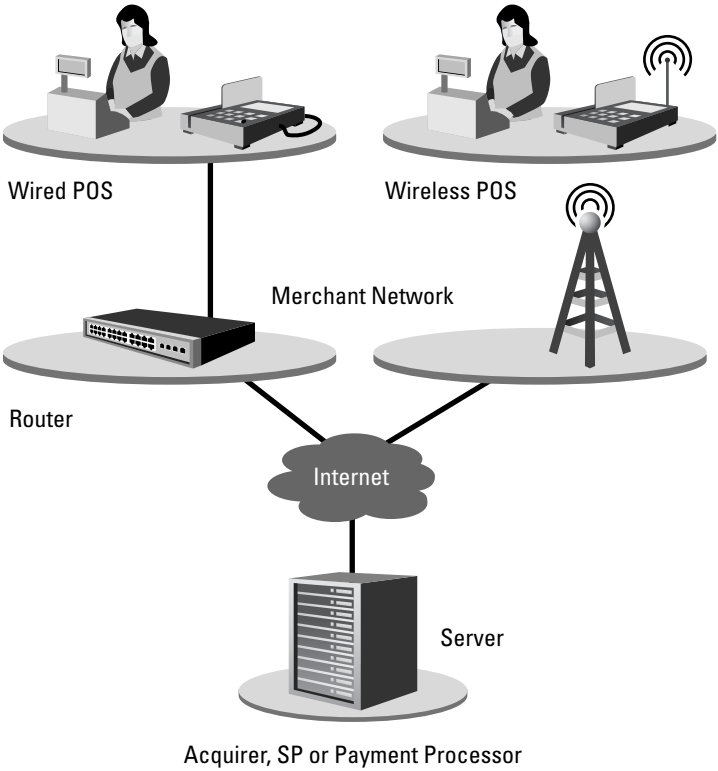


Figure 3-2: The primary domains of PCI security responsibility for a merchant.

Two Kinds of PCI Requirements: Technology and Process

The PCI Data Security Standard specifies two kinds of tools or controls for fixing the vulnerabilities mentioned in the previous section and securing cardholder data. They are *technology* and *process*:

- Security technology consists of software, hardware and third-party services used to implement purpose-built applications that protect cardholder data from various threats.
- Security process is a specific set of operational procedures used to implement and maintain protection, which may or may not require a particular type of security technology.

Quite often, though, technology and process go hand-in-hand.

For example, every merchant needs to stop malware such as viruses, worms, and spyware from breaching cardholder data. The PCI-approved solution for malware entails both technology *and* process:

- **Technology:** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
- **Process:** Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Merchants must devote ongoing attention to PCI. Compliance with PCI isn't a one-shot event – it demands *continuous monitoring* of all security technologies and processes for protecting cardholder data. But the benefits are worth the effort.

As we explained in Part I, the PCI Data Security Standard has six major goals with 12 associated requirements. In the next sections, we explain the PCI requirements, condensed from the official standard. (The information in this book does not replace granular requirements in the actual standard. Consult

PCI DSS Requirements and Security Assessment Procedures for full details. A copy is posted at the PCI Security Standards Council website: `www.pcisecuritystandards.org`.)

Build and Maintain a Secure Network

The network is the glue connecting payment card terminals, processing systems, and retail commerce in general. By exploiting network vulnerabilities, a criminal can access cardholder data much more easily than when thieves had to gain physical access to your building and systems. The Internet and web were never designed with security as a core requirement, so it's vital that merchants implement PCI controls to secure their internal networks, and links through external networks to third-party service providers who process cardholder data. Toward this end, the PCI Data Security Standard provides the following two requirements for network security.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The firewall is a fundamental security tool that every merchant must use when cardholder data on the internal network is potentially exposed to the Internet. In the world of networking, a *firewall* controls the passage of electronic traffic within your internal network and between internal and external networks. Using a firewall on your network has the same value as using mechanical locks on doors to your physical business. Firewalls keep the bad guys out.

Firewall capability is often built into another device called a *router*, which is hardware or software that provides connection functionality for traffic flowing between networks. For example, most Wi-Fi routers for wireless hotspots include a firewall.

PCI requires the use of a firewall, but it also asks merchants to use appropriate processes to ensure that the firewall effectively blocks malicious traffic. PCI requires you to use firewall and router configuration standards that must be tested every time you change equipment or software configurations. These must be reviewed at least every six months. Merchants need to be aware of all connections to cardholder data – including wireless. Your firewall configuration must deny all traffic to the cardholder data except for authorized users and uses.

Your firewall configuration must prohibit unauthorized access to system components in your cardholder data environment. Access to non-essential system components and ports should also be blocked. Be sure to install personal firewall software on each mobile and/or employee-owned computer that connects to your cardholder data environment or to the public Internet.

Follow this requirement and you'll have fixed a major exposure to cardholder data!

Requirement 2: Don't use vendor-supplied defaults for system passwords and other security parameters

It's vital for merchants to ensure strong passwords are used for PCI security. Doing so may seem obvious, but the easiest way for hackers and criminals to breach your cardholder data is by guessing the right password.

When software and hardware comes out of the box, the passwords are set to a default value. The most common security error by merchants who deploy these is to not change default passwords. Default passwords are easily retrieved with a search engine, so leaving them intact is like giving thieves a master key to access your cardholder data. Yikes!

Table 3-1 shows typical default passwords that you need to change *before* you deploy any infrastructure used with cardholder data.

Table 3-1	Typical Default Passwords to Change Before Deployment
[no password]	manager
[name of product or vendor]	pass
1234 or 4321	password
access	root
admin	sa
anonymous	secret
database	sysadmin
guest	user

The PCI Data Security Standard directs merchants to develop configuration standards for all system components that address all known vulnerabilities. This includes changing default passwords for wireless devices that link to the cardholder data environment or are used to transmit cardholder data. PCI says you need to encrypt all 'non-console administrative access' – such as when using a browser to manage a wireless router. The next section explores encryption and other ways to ensure the security of cardholder data.

Protect Cardholder Data

The goal of protecting cardholder data is at the heart of PCI. Various technical methods of protecting cardholder data exist, such as encryption, truncation, masking and hashing. But you don't have to be a tech guru to understand their purpose: to make cardholder data *unreadable* to unauthorized people. Even if a thief manages to smash through security controls and obtain cardholder data, the information will have no value because the thief will be unable to read and use it.

We gave a general description of cardholder data at the beginning of Part II, but this is a good place to dive deeper and clarify exactly what merchants must protect to comply with PCI requirements.

Cardholder data is any information printed on or stored on a payment card. Digital storage is on the magnetic stripe on the back of a card, or in a chip embedded on the front of some cards. The Primary Account Number (PAN) is the most prominent cardholder data, along with the cardholder's name, service code and expiration date. In addition to these, sensitive authentication data must be protected. The cardholder data we mean here is data that's processed or stored in the merchant's information technology infrastructure, and data transmitted over open, public networks like the Internet.

Table 3-2 summarizes cardholder data elements and sensitive authentication data, plus the security guidelines required (data such as PIN numbers should never be stored, so protection by the merchant isn't applicable).

Table 3-2 Cardholder Data Elements and PCI Security Guidelines

Type of Data	*Data Element*	*Storage Permitted*	*Protection Required*	*Rendered Unreadable**
Cardholder Data	Primary Number Account (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2 / CVV2 / CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

** Per PCI DSS Requirement 3.4.*

Requirement 3: Protect stored cardholder data

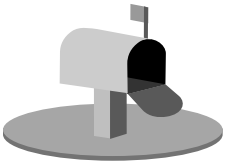
If you don't store cardholder data, it's easy – compliance with this PCI requirement is automatic. PCI compliance requires merchants to keep cardholder data storage to a minimum, and to create a retention and disposal policy limiting this practice to the minimum required for business, legal, and/or regulatory purposes. *Never* store sensitive authentication data (detailed in Table 3-2). Some merchants do so at great risk to customers and to themselves. Don't fall into this trap – if you don't need it, don't store it!

A typical place where merchants electronically gather and inappropriately store cardholder data is the card-not-present purchase done via mail, telephone, or a web-based e-commerce application. Figure 3-3 shows the tools and controls used to authenticate these purchases. Non-compliance with PCI begins when a merchant stores these data. Ironically, breaches have occurred where the merchant wasn't even aware that these data had been stored. Analyze your business's card processing applications to find out exactly where cardholder data resides at all times, and eliminate storage of all sensitive data after authentication. Sensitive authentication data may *not* be stored at any time, *even if encrypted*.

The PCI Data Security Standard provides guidelines for cardholder data that you can store. Aside from employees who may have a legitimate business reason to see a cardholder's full PAN, *a merchant must always mask display of this number*. In other words, the most you can show are the first six and last four digits. This restriction doesn't supersede stricter requirements for displaying PAN on a point-of-sale receipt.

Card-Not-Present Merchant

Payment Channels



Mail

Telephone

E-Commerce

Controls

- CID, CAV2, CVC2, CVV2
- AVS
- 3D Secure
  (Verified by Visa, MasterCard's Secure Code, JCB's J/Secure)

Figure 3-3: Controls for authorizing and validating card-not-present purchases.

Merchants must always render PAN unreadable wherever it's stored, including backup media, in logs, on portable digital storage devices, and via wireless networks. Permissible technology solutions for masking PAN include:

- Strong one-way hash functions or a hashed index, which shows only index data that point to database records containing the PAN.
- *Truncation*, which deletes a forbidden data segment and shows only the last four digits of the PAN.
- Strong cryptography and associated key management processes and procedures. Cryptographic keys must be protected from disclosure and any misuse documented by the merchant.

Understanding strong cryptography

Cryptography is a complex mathematical process of making plaintext data unreadable to people who don't have special knowledge in the form of a 'key' to unlock the data. Encryption transforms plaintext into ciphertext, while decryption changes ciphertext back into plaintext. Cryptography may be used on data that's stored or transmitted over a network.

Strong cryptography is extremely resilient to unauthorized access – provided that the key isn't exposed. The strength of a cryptographic formula relies on the size of the key. The key you use needs to meet the minimum size suggested by several industry recommendations. A good public reference is the National Institute of Standards and Technology (NIST) Special Publication 800-57 (find it at `http://csrc.nist.gov/publications/PubsSPs.html`). You may need technical assistance to implement strong encryption but commercial and public domain solutions are available. Options that meet minimum key bit security requirements include:

- 80 bits for secret key based systems (such as 3DES)
- 1024 bits modulus for public key algorithms based on the factorization (such as RSA)
- 1024 bits for the discrete logarithm (such as Diffie-Hellman) with a minimum 160 bits size of a large subgroup (such as DSA)
- 160 bits for elliptic curve cryptography (such as ECDSA)

(Source: PCI DSS Glossary)

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Cardholder data that moves across open, public networks must be encrypted to protect it from being compromised by thieves. PCI requires you to use strong cryptography and security protocols such as SSL/TLS or IPSec to protect sensitive cardholder data during transmission. Examples of open, public networks include the Internet and email, wireless hot spots, global system for mobile communications (GSM) and general packet radio service (GPRS).

New changes to this encryption requirement focus on upgrading the security of wireless networks transmitting cardholder data, or connecting to the cardholder data environment. PCI suggests using the industry standard best practices (IEEE 802.11x, for example) to implement strong encryption for authentication and transmission. New wireless implementations are prohibited from using WEP (Wireless Equivalent Privacy) after March 31, 2009 because it's known to be insecure. Current wireless implementations are prohibited to use WEP after June 30, 2010.

Never send unencrypted PANs with end-user messaging technologies such as email, text messaging, instant messaging or chat.

Maintain a Vulnerability Management Program

Vulnerability management is a process that every merchant can use to avoid exploiting weaknesses in your card payment infrastructure. New vulnerabilities appear every day due to flaws in software, faulty configuration of applications and IT gear, and (dare we say it?) good old human error. Whatever their source, vulnerabilities don't go away by themselves. Their detection, removal, and control require vulnerability management. VM, as vulnerability management is called, is the regulated, continuous use of specialized security tools and workflow that actively help to eliminate exploitable risks. Every merchant can benefit from a comprehensive VM program to protect cardholder data. Typical VM workflow includes these steps:

- Ensuring that security policies for cardholder data work with the VM process.
- Tracking IT inventory and categorizing assets to help prioritize the elements most critical for safeguarding cardholder data.
- Scanning systems for vulnerabilities (more on this later in the section 'Requirement 11: Regularly test security systems and processes').

- Verifying vulnerabilities against inventory to weed out false positive indications of weak points.
- Classifying and ranking risks.
- Pre-testing and applying patches, fixes, and workarounds.
- Rescanning to verify compliance.

In the next sections we describe two specific requirements of PCI for vulnerability management.

Requirement 5: Use and regularly update anti-virus software or programs

Anti-virus software comes up a lot in discussions about IT security, and for good reason. Vulnerabilities such as malware, viruses, Trojan horses and worms often inject themselves into a cardholder data system by means of email and other common online activities undertaken by your employees. Anti-virus software is the technology used to limit this 'risk vector' to protect cardholder data.

REMEMBER

PCI requires merchants to use anti-virus software on all systems that touch the cardholder data environment, which may be affected by malicious software. The risk is especially high for personal computers and mobile devices that plug into the cardholder data environment. Servers are another high-priority risk that need anti-virus protection.

TIP

The process portion of the anti-virus requirement is to ensure that the technology you deploy is the current version, is always running on every affected device, and can generate audit logs to help auditors verify compliance during a PCI assessment or forensic analysis. Without audit logs, you could be unaware of an unauthorized browser extension or malware that reads PANs as they're entered into a payment application.

Requirement 6: Develop and maintain secure systems and applications

Data thieves frequently exploit vulnerabilities within the cardholder data system and its applications. So when you purchase payment applications and devices used to accept card payments (it would be most unusual for a small merchant to be creating these from scratch), you need to buy only those payment applications and devices that are approved by the PCI Security Standards Council. Lists of each are posted on the Council website.

Manufacturers and developers must follow guidelines of the PA DSS and PIN Entry Device Security Requirements to lock down those attack vectors. The specifications in Requirement 6 are primarily for organizations that develop their own custom payment applications. Whether you develop in-house payment applications or buy them from someone else, the development process needs to use secure coding best practices such as Open Web Application Security Project (OWASP).

TIP

Vulnerabilities in systems and applications may occur over time as data thieves discover ways to subvert what was once secure. Security patches for payment applications developed in-house must be devised by your organization. You must install vendor-supplied security patches to eliminate vulnerabilities. Think of these as a quick-repair job addressing a specific section of programming code prone to error.

New vulnerabilities appear every day so merchants must do frequent audits and repair weaknesses as soon as possible. The process of patching requires merchants to employ several strategies to keep systems and applications secure. In a nutshell:

TECHNICAL STUFF

- Install the most recently-released patch for critical card payment systems and applications within one month of release.
- Apply patches to less-critical systems as soon as you can, based on priorities established by your vulnerability management program.

- Follow a process to ensure you don't overlook a new vulnerability. A vulnerability scanning service can provide you with this information automatically.
- If you develop your own payment applications, follow industry best practices that incorporate security into the entire software development lifecycle.
- Follow change control procedures whenever you change payment card system components or configurations.
- Follow secure coding guidelines for web applications and use a process to review custom application code for coding vulnerabilities. Web applications are particularly susceptible to exploitation of vulnerabilities such as remote code execution, SQL injection, format strings, cross-site scripting, and username enumeration.
- To secure your public-facing web applications, make sure you regularly use specialized web application testing tools or methods. Optionally, you can also install a web application firewall.

Implement Strong Access Control Measures

The essence of *access control* is simple: it enables merchants to permit or deny the physical or technical means to access PAN or other cardholder data. Access control is so crucial for PCI that it's the only goal in the Data Security Standard with three separate requirements. These provide merchants with a comprehensive strategy for implementing strong access control:

- The first requirement ensures that cardholder data can be accessed only by employees with a business need-to-know – no snooping allowed!
- The second addresses logical access pertaining to PIN entry devices, payment applications, networks, PCs and other computing gear used to view cardholder data.
- The third requirement addresses physical access such as locks and other security measures used to protect paper-based records and cardholder system hardware.

Requirement 7: Restrict access to cardholder data by business need-to-know

Segregating access rights is nowhere more crucial than with cardholder data. PCI requires merchants to ensure that employees are granted access rights to the *least* amount of data they need to perform a job. To put it bluntly, if an employee doesn't need access to cardholder data, the employee must not have access.

To implement this requirement, you need to establish an access control system for each element of the cardholder data infrastructure, based on a user's need-to-know. All access rights must be set by default to 'deny all' unless an individual is specifically allowed access to designated cardholder data – no exceptions!

Requirement 8: Assign a unique ID to each person with computer access

The intent of Requirement 8 is to aid forensic analysis of cardholder data access that permits a merchant to trace every action of electronic access to a specific worker. To do this, PCI specifies the following:

- You must assign each worker a unique user name before granting access rights to cardholder data system components or the data itself.
- Each user must be authenticated to access the system by using a password or passphrase, or two-factor authentication (see the nearby sidebar, 'Feeling the power of Strong Authentication' for an explanation).
- For all remote access to the network, you need to implement two-factor authentication. The standard suggests using a remote authentication and dial-in service, a terminal access controller access-control system with tokens, or a virtual private network (VPN) with individual certificates.

- You must make all passwords unreadable for each cardholder data system component – both in storage and during transmission – using strong cryptography based on approved standards.
- For non-consumer users and administrators, be sure to use proper user authentication and password management on all system components.

Feeling the power of 'Strong Authentication'

Authentication is the process of verifying a device or a person for security purposes. Traditional authentication has been *single factor*, which means only one piece of information was required to complete authentication.

Multi-factor authentication raises the bar by requiring two or more 'factors' or pieces of information to complete authentication. When a merchant uses multi-factor authentication, experts call this 'strong authentication'.

An authentication factor usually falls into one of three types:

- Something a user *has*, such as an ID card, a device or security token, or a telephone.
- Something a user *knows*, such as a password or passphrase, a key sequence, or a personal identification number (PIN). A secure pass code must include at least seven alpha and numeric characters, and be changed at least once every 90 days.
- Something a user *is* or *does*, which usually is a fingerprint, retinal pattern, voice pattern, signature, or DNA sequence.

For example, in-person payment card authentication requires two factors. First, a user presents the physical card with its associated PAN, and then the user enters the PIN. Authenticating a card-not-present transaction requires presentation of three factors: the PAN, the card expiration date, and the three-digit CAV2/CID/CVC2/CW2.

The PCI Data Security Standard requires you to have employees use two-factor authentication for accessing cardholder data. The employee must also meet the precondition of being authorized to access cardholder data as a job function requirement. By using strong authentication, you can fulfill PCI Requirement 8 and help protect cardholder data.

Requirement 9: Restrict physical access to cardholder data

Lest you forget about 'old fashioned' non-digital security, PCI also instructs merchants to restrict physical access to cardholder data or systems that house cardholder data – including hardcopies. This provision has 10 sub-requirements:

- Limit and monitor physical access to systems in the cardholder data environment with facility entry controls.
- Use video cameras to monitor entry and exit points of your cardholder data storage facility, and store the footage for at least three months. Surveillance is not required for point-of-sale locations.
- Use badges or other procedures to help all workers easily tell the difference between an employee and a visitor – especially in the cardholder data environment.
- Authorize all visitors before admitting them to areas where cardholder data is processed. Give visitors a physical token that expires and clearly identifies them as non-employees. Visitors must surrender the physical token before they leave the facility or upon expiration.
- Retain visitor information and activity in a visitor log for audit purposes, and retain it for at least three months unless restricted by law.
- Store media backups of cardholder data in a secure location (preferably offsite).
- Ensure that all paper and electronic media with cardholder data is physically secure.
- Strictly control the distribution of any media with cardholder data – both to internal and external recipients.
- Formally approve any movement of media with cardholder data from a secured area, – especially when it goes to individuals.
- Strictly control the storage and accessibility of media with cardholder data.
- Be sure to destroy media with cardholder data when you no longer need it for business or legal reasons.

Regularly Monitor and Test Networks

Your network is one of the most important elements in the cardholder data environment. Physical and wireless networks enable the flow of cardholder data from PIN entry devices and PCs to servers, payment applications, storage media, and onward to the third-party processor or acquiring bank. A vulnerability existing at any point of the network spells trouble if a data thief exploits it for unauthorized access to cardholder data.

New vulnerabilities appear every day. Merchants must regularly monitor and test all of their networks to find and fix vulnerabilities before trouble occurs.

Requirement 10: Track and monitor all access to network resources and cardholder data

This requirement is all about system activity logs. Logging mechanisms are critical for vulnerability management and forensics. If something goes wrong, only a log can provide the data you need to determine who did what, when it happened, and what needs to be fixed. For this reason, merchants must create a process that links all access by individual users to cardholder system components – especially when done with administrative privileges.

Your IT staff has a big role for meeting this requirement. IT must implement automated audit trails for monitoring and tracking. Recording the operational minutia is the only way to reconstruct events in question. You may be required to show investigators individual user accesses to cardholder data. Documentation may be required for all actions taken by anyone with root or administrative privileges – with precise audit trails. Merchants must be able to show details such as invalid logical access attempts, use of identification and authentication mechanisms, initialization of audit logs, and creation and deletion of system-level objects.

The ability to produce detailed audit reports on demand is important for PCI. The standard requires the following:

- You have entries for all system components for each event.
- You ensure a minimum level of detail that includes user ID, type of event, date, time, success or failure indication, origination of event, ID or name of affected data, system component or resource.
- All system clocks/times are synchronized.
- Audit trails are impervious to alteration.
- The logs for security-related functions of every system component are reviewed at least daily.
- You store the audit trail history for at least one year. Three months of data must be immediately available for analysis.

Requirement 11: Regularly test security systems and processes

New vulnerabilities are discovered daily but that's no reason to be paralyzed with dread. PCI requires merchants to regularly test cardholder data systems and processes in order to systematically find those vulnerabilities and fix them. Items to test include wired and wireless networks, network gear, servers, other system components, processes, and custom software. Testing must be frequent, and is vital right after you make big changes such as deploying new software or changing a system configuration.

Threats come from inside and outside so you need to test both your internal and external networks every 90 days.

How to test?

Vulnerability scanning products and services enable you to scan automatically and fulfill PCI testing requirements. You need to use an Approved Scanning Vendor (ASV) to scan your external network. A list of ASVs is available at

www.pcisecuritystandards.org. A Qualified Security Assessor may audit all 12 requirements of PCI, but can't do network scans unless it is also an ASV.

What to test?

PCI requires at least quarterly scans of your cardholder data network, including wireless. Follow these points:

- For wired networks, use an ASV to scan your external network. Internal networks may be scanned by your in-house staff with scanning tools.
- For wireless networks, use a wireless analyzer or wireless intrusion detection service or intrusion prevention service (IDS/IPS). You must be able to identify *all* wireless devices to control their access to the cardholder data environment.
- IDS/IPS is also required to monitor all other traffic in the cardholder data environment. Alerts should notify security specialists immediately. You need to keep security software up to date.
- Use file integrity monitoring software. This alerts you to unauthorized changes to critical system files, configuration files, and content files. Compare critical files at least weekly.

When to test?

Merchants must scan their internal and external networks at least quarterly, and always right after making a big change to the network. You're not required to hire an ASV to do internal scans, but must have one to do external scans. Merchants must do internal and external penetration testing ('pen test') at least annually. A *penetration test* is a controlled attack on your cardholder data environment. Merchants must also do a pen test after a big change to the cardholder data environment.

Humane Society of the US case study

Industry: Not-for-profit

Headquarters: Washington, DC

Business: Leading animal protection non-profit that fights for the protection of animal rights through advocacy, education, legislation, and hands-on programs

Size: The nation's largest animal protection organization with 10+ million members and constituents

'By turning to QualysGuard PCI, we significantly save on the time and resources we need to dedicate to maintaining PCI compliance.' – Chief Information Officer

Objectives:

- The Humane Society had maintained a secure network, but continuously maintaining PCI compliance was costly and time-consuming.
- The organization needed a streamlined way to complete the required PCI DSS questionnaires and network vulnerability audits, and validate compliance to its acquiring banks.

Results:

- QualysGuard PCI helps the Humane Society to automatically validate its PCI DSS compliance and it's now able to quickly complete PCI DSS Self-Assessment Questionnaires.
- QualysGuard enables the Humane Society to document and submit proof of compliance to acquiring banks.
- The Humane Society can protect its member and contributor information with help from QualysGuard.

Take a look at `www.qualys.com/customers/success/` for more info and other case studies.

Using the tests

When you scan for vulnerabilities, the report presenting scan results need to provide a clear, overall, pass/fail as well as a pass/fail for each individual component. The pass/fail is determined by the ASV based on requirements set by the PCI Council. The report should classify the information with the Common Vulnerability Scoring System to help prioritize remediation. The Council publishes this example:

- **5 Urgent:** Trojan horses, file read and write exploit, remote command execution.
- **4 Critical:** Potential Trojan horses, file read exploit.
- **3 High:** Limited exploit of read, directory browsing, denial of service.
- **2 Medium:** Sensitive configuration information can be obtained by hackers.
- **1 Low:** Information can be obtained by hackers on configuration.

Maintain an Information Security Policy

A merchant organization needs to govern all PCI security activity with clear security policies. The policies make it easier to create and follow your PCI compliance program. The result of good policies makes it easier and faster for your IT security team to discover vulnerabilities in the cardholder data environment, remediate those security holes, and produce documentation to satisfy requirements for compliance.

Policy-making starts at the top of an organization, and must flow through to each worker so that everyone understands their role in protecting cardholder data.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

Your security policies determine the nature of the controls used to ensure security and comply with PCI requirements. The policies and controls need to apply to everything in the cardholder data environment – PIN entry devices, PCs and other endpoints, servers, network services, applications, and the people who use them.

The PCI Data Security Standard requires merchants to maintain a policy that addresses information security for employees and contractors. The following list adapts text from nine areas of the standard that must be established, published, maintained, and disseminated to everyone affected by the policy:

- **Comprehensive formal policy:** Your security policy must address all PCI requirements. You need a process to identify vulnerabilities and assess risk, with at least an annual review. Reviews must be conducted when a cardholder environment changes.
- **Daily procedures:** Be sure your daily operations procedures meet PCI requirements.
- **Usage policies:** Employees and contractors must have usage policies for each technology they use that affects the cardholder data environment. This would include handheld devices and laptops, removable electronic media, Internet, wireless, remote access, email and other applications.
- **Clear responsibilities:** Employees and contractors must clearly understand their information security responsibilities.
- **Assigned responsibilities:** Assign responsibilities to specific individuals, such as someone to receive and respond to security alerts, or someone who should monitor and control access to data.

- **Security awareness program:** Your business must formally teach employees the importance of cardholder data security.
- **Employee screening:** You need to screen every employee before hiring to help limit security risks from inside your business.
- **Third-party services screening:** If you share cardholder data with a third-party service provider, they must also comply with PCI.
- **Incident response plan:** Be prepared with a detailed plan for immediate response to a breach.

Compensating Controls for PCI

Many merchants face legitimate business and technical constraints related to specific PCI requirements. To acknowledge this fact of business life, the PCI Data Security Standard includes an appendix called Compensating Controls. The idea is to give merchants a measure of flexibility in following a particular control in PCI DSS, provided the merchant has sufficiently mitigated the risk with a compensating control.

Compensating controls aren't automatically approved. They must meet these criteria:

- Provide identical 'intent and rigor' of the PCI requirement.
- Provide identical level of security defense as the PCI requirement.
- Be 'above and beyond' other PCI requirements. This means existing PCI requirements cannot also serve as compensating controls if they're already required for the item under review. They may be considered if they're required somewhere else, but not for the item under review. You may also combine existing PCI requirements and new controls as a compensating control.
- Be effective enough to meet additional risk created by not following the PCI requirement.

The use of compensating controls allows merchants some measure of flexibility in complying with PCI. But merchants must still be able to pass an annual assessment by a Qualified Security Assessor according to the standards set in PCI DSS Appendix B. As with all PCI requirements, processes and controls must assure continuous use of compensating controls after each annual assessment.

Our summary of PCI requirements should give you a solid grasp of how to comply with the standard. You can find full details of each requirement in *PCI DSS Requirements and Security Assessment Procedures* at `www.pcisecurity standards.org`. In Part IV, we describe the actual process of what a merchant can do to comply with PCI DSS.

Part IV

Verifying Compliance with PCI

In This Part

- Understanding the formal process of compliance
- Preparing for a PCI onsite compliance assessment
- Choosing a Qualified Security Assessor or an Approved Scanning Vendor
- Using a Self-Assessment Questionnaire

The PCI Data Security Standard must be met by merchants – and indeed, *any* organization – that stores, processes or transmits cardholder data. While the PCI Security Standards Council manages the standard, the card brands do the actual enforcement. Each brand has its own cardholder data security compliance program, but all brands endorse PCI DSS and recognize its requirements as meeting their own technical requirements.

Each card brand still has a few unique requirements for compliance. These mainly deal with merchant classification levels and rules for self-assessment, such as when to use a Qualified Security Assessor. Consult these links for specific card brand compliance programs:

- **American Express:** `www.americanexpress.com/datasecurity`
- **Discover Financial Services:** `http://discovernetwork.com/fraudsecurity/disc.html`
- **JCB International:** `www.jcb-global.com/english/pci/index.html`

- **MasterCard Worldwide:** www.mastercard.com/sdp
- **Visa Inc:** www.visa.com/cisp (US)

Following the Process of Compliance

The most important idea to remember about PCI compliance is your merchant level number. The *level* determines the degree of rigor that your organization will be subjected to for purposes of verifying PCI compliance. The levels are based on criteria published by the card brands, and there are a few differences from one card brand's compliance program to another.

For purposes of illustration, Table 4-1 shows the typical merchant levels and criteria. (Please consult specific card brand compliance programs for exact specifications.)

Level 2 to 4 merchants must complete an annual Self-Assessment Questionnaire (SAQ) and an Approved Scanning Vendor (ASV) must do a quarterly scan of the cardholder data network. If you use compensating controls, you need to include that documentation with your *Report on Compliance* (described in the later section 'Meeting the Reporting Requirements of PCI DSS'). Level 2 to 4 merchants don't require an annual onsite assessment, except in some cases such as after suffering a breach of cardholder data. On-site assessments must be completed by a Qualified Security Assessor (QSA). Later in this Part, we describe how to choose a QSA and ASV, and how merchants can select and use a SAQ.

For most merchants, the formal process of PCI compliance consists of submitting the annual SAQ and quarterly ASV-generated network scan reports. However, if your organization is required to have an annual security assessment, you need to follow other steps in the process of PCI compliance. Read on!

Table 4-1: Typical Card Brand Merchant Levels and Validation Actions

Level	*Criteria*	*On-Site Security Audit*	*Self-Assessment Questionnaire*	*Network Scan*
1	Any merchant, regardless of acceptance channel, processing **more than 6 million transactions** per year. Any merchant that suffered a security breach resulting in cardholder data compromise.	Required annually.		Required quarterly.
2	Any merchant processing **between 1 to 6 million** transactions per year.		Required annually.	Required quarterly.
3	Any merchant processing **between 20,000 to 1 million transactions** per year.		Required annually.	Required quarterly.
4	**All other merchants** not in Levels 1, 2 or 3, regardless of acceptance channel.		Required annually.	Required quarterly.

Preparing for a PCI On-site Assessment

Depending on the complexity of your cardholder data environment, an onsite PCI security assessment requires active preparation, coordination and follow-up. Your organization needs to designate a project manager to coordinate the process with internal resources and the Qualified Security Assessor (QSA) – especially during onsite visits. Preparation can smooth execution and help ensure a successful assessment. Here's a list of the advance preparation you need to do:

- Coordinate internal resources and availability including IT security, networking, infrastructure, payment card application owners, legal, human resources and executive management.
- Create timelines and internal reporting mechanisms.
- Document everything related to your cardholder data environment including security policies, network diagrams, change control procedures, and log files specified by PCI DSS. Include PCI letters and notifications.
- Describe compensating controls and why they were selected, the business and technical reasons for the particular implementation and deployment, and performance and results.
- Describe the cardholder data environment, especially the cardholder data flow and location of cardholder data repositories.

The Qualified Security Assessor requests these documents during the onsite PCI compliance assessment. The process includes interviews and inspections of the physical and logical cardholder data infrastructure. An assessment usually follows five steps.

Step 1: Scoping

Scoping is the process of specifying exactly what is tested for compliance. It limits the PCI assessment to security technology and processes affecting the security of cardholder data. A

merchant can leverage *network segmentation* – to effectively isolate systems that store, process, or transmit cardholder data from the rest of the network. For purposes of PCI compliance, controls are required only for the affected segments. In the practical world, most merchants would probably want to extend security controls to their entire IT infrastructure to ensure comprehensive protection beyond the letter of the law.

Step 2: Sampling

During a PCI assessment, sampling is where the QSA selects a subset of in-scope security controls and processes. Compliance tests are done only on the subset. Sampling is allowed because examining and testing every single control and process is a little impractical! (You can find a flowchart for scoping and sampling in PCI DSS Appendix F at `www.pcisecuritystandards.org`.)

Step 3: Verifying compensating controls

If you've investigated a particular risk associated with PCI and elected to deploy a compensating control, the QSA will examine the compensating control and weigh your arguments for its alternative deployment. The QSA may test the compensating control to verify its effectiveness. The QSA must 'OK' the compensating control in order for you to pass the assessment for PCI compliance.

Step 4: Reporting

Reporting includes four steps:

- The QSA completes a formal document called the *Report on Compliance (ROC)*.
- You attach evidence of passing four quarterly vulnerability scans from an Approved Scanning Vendor.
- You complete the *Attestation of Compliance* (see the copy in PCI DSS Appendix D on the website).
- You submit the three documents to your acquirer or payment card brand.

Step 5: Clarifying

Sometimes the acquirer or payment brand may ask you for clarification on a point covered in the Attestation of Compliance. You must meet requests for clarification to be compliant with PCI.

Choosing a Qualified Security Assessor

Sometimes a merchant must hire a Qualified Security Assessor (QSA) in order to be certified as compliant with the standard. The PCI Security Standards Council website posts a list of QSAs, which are data security companies that are trained and certified to do onsite assessments that verify compliance with PCI DSS. A merchant's choice of the QSA is important to getting certified for compliance with the standard.

Aside from the usual customer testimonials on a QSA website, be sure to check out the QSA's business culture. Will it fit with the culture of your own organization? Seek a QSA that knows how your business works. Their experience with your standard processes will help make the assessment go more smoothly and quickly and will be invaluable for understanding the rationale of your compensating controls.

The QSA's job is to verify your documentation, and technical and process controls for adherence to the *PCI DSS Requirements and Security Assessment Procedures* (see the Council's website for a copy). The QSA will define the scope of your assessment and select systems for sampling. Ask the QSA to describe its standard density formula and how that produces a sample. Find out how the QSA will assess your cardholder data environment, such as by function or technology.

The QSA will produce your final report called the *Report on Compliance (ROC)*, which you must submit to your acquirer or payment card brand.

Your organization might ask the QSA to do other security-related custom services, such as a penetration test or a PCI gap assessment. This is another reason to look for a good fit to ensure a successful long-term engagement.

QSAs aren't allowed to require any particular product or vendor as a condition to certify compliance. The QSA must accept a scan report from any ASV. The QSA is also required to provide you with a feedback form, which you can send to the PCI Council.

Selecting an Approved Scanning Vendor

External Network scanning is done with vulnerability assessment tools that are created or used by an Approved Scanning Vendor (ASV). The ASV may perform the scans for the merchant or provide a self-service web-based network vulnerability scanning solution specifically for PCI scanning. You can find a list of Approved Scanning Vendors posted on the Council website.

If false positives appear in the scanning process, the ASV works with the merchant to analyze report results, and grant appropriate exceptions with clarifying documentation.

When choosing an ASV, pick one that can help you meet compliance requirements and help your organization become more secure. Beware of an ASV that's too eager to grant your organization with a passing score just to get your business – this ploy may do more harm than good if actual vulnerabilities aren't identified or remediated to produce real security.

The ASV scanning solution must meet several preconditions to be approved for use by merchants:

- **Non-disruptive:** When conducting a scan, the solution must never interfere with the cardholder data system. For example, you wouldn't want the scanning process to trigger a system reboot, nor would you want it to conflict with domain name server (DNS) routing.
- **No stealth installations of software:** The scanning solution must never install a root kit or other software application unless you're aware in advance that this is part of the scanning process, and this is pre-approved by you.

- **Excludes dangerous tests:** The ASV solution is forbidden from overloading bandwidth or launching tests that could cause catastrophic failure, including denial of service, buffer overflow, or a 'brute force' attack that triggers a password lockout.
- **Fulfills PCI reporting:** A scan report produced by the ASV solution must conform to the standard's requirements.

Using the Self-Assessment Questionnaire

For the majority of merchants, a Self-Assessment Questionnaire (SAQ) is adequate to evaluate their compliance with PCI DSS rather than an onsite assessment by a Qualified Security Assessor. To help ease the process of doing a self-assessment, the PCI Security Standards Council has produced different SAQs that are tailored for specific operating situations.

Table 4-2 presents the five types of SAQ validations and corresponding descriptions of how you might accept payment cards, such as for card-not-present transactions or use of standalone dial-up terminals. Use the corresponding SAQ, which is labeled A, B, C or D. All SAQs are posted on the Council website.

Table 4-2 Self-Assessment Questionnaires for Different Merchant Requirements

SAQ Validation Type	*Description*	*SAQ*
1	Card-not-present (e-commerce or mail/telephone order) merchants, where all cardholder data functions are outsourced. (This never applies to face-to-face merchants.)	A
2	Imprint-only merchants with no cardholder data storage.	B
3	Standalone dial-up terminal merchants with no cardholder data storage.	B

(continued)

Table 4-2 ***(continued)***

SAQ Validation Type	*Description*	*SAQ*
4	Merchants with payment application systems connected to the Internet, and no cardholder data storage.	C
5	All other merchants (not included in descriptions for SAQs A, B or C above), and all service providers defined by a payment brand as eligible to complete a SAQ.	D

Source: PCI Security Standards Council

Meeting the Reporting Requirements of PCI DSS

Your acquirer or requesting card brand will require, at a minimum, the annual compliance report plus quarterly network scan reports. Depending on requirements, the annual report will either be the appropriate Self-Assessment Questionnaire or the *Report on Compliance (ROC)* along with the *Attestation of Compliance for Onsite Assessment – Merchants*. Check the PCI DSS compliance programs of each card brand for unique additional requirements.

The *Report on Compliance* includes the following content and format:

- **Executive Summary.** Describes, in a nutshell, the essence of findings related to security of cardholder data.
- **Description of Scope of Work and Approach Taken.** This includes the environment tested, information on network segmentation, sampling data, associated entities tested, wireless LANs and payment applications tested, version of PCI DSS used for the assessment, and the timeframe.

Remaining vigilant

The process of PCI compliance isn't a do-it-and-forget-about-it event. The formality of filing an annual Self-Assessment Questionnaire and quarterly network scans only captures a snapshot in time. And that's what certification of compliance is: a statement that the merchant was in compliance when the reports were submitted. New risks to cardholder data security, however, arise daily, so merchants need to ensure the ongoing and continuous implementation of controls and processes specified by PCI. An ongoing compliance program consists of three elements: Assess, Remediate, and Report.

Assess

Regularly asses the security of your network and cardholder data environment, and frequently scan the network for vulnerabilities – always do so after major changes occur in the cardholder data processing environment. It's crucial to examine security log files every day to monitor access and usage of cardholder data. PCI requires that stored log data is immediately available for analysis.

Remediate

You need to quickly fix vulnerabilities that threaten the security of cardholder data. Test new patches and deploy them as soon as possible to minimize potential exploits. Stay vigilant with business processes related to cardholder data security. Just one innocuous change might accidentally place cardholder data outside of protective PCI controls.

Report

PCI security reports enable you to review the effectiveness of PCI controls and processes. Reports also help you prioritize remediation activity. By regularly consulting reports, your organization will have continuous visibility on the state of PCI security and compliance. Ongoing use of this tool helps ensure the success of a merchant's annual compliance assessment.

- **Details about Reviewed Environment.** This includes a diagram of each network segment tested, a description of cardholder data environment, lists of hardware and critical software, service providers, third-party payment applications, individuals interviewed and titles, and the documentation reviewed.
- **Contact Information and Report Date.** This includes contact information for the merchant and assessor, and the date of report.

- **Quarterly Scan Results.** This includes a summary of the four most recent quarterly scan results.
- **Findings and Observations.** This includes a summary of any findings that may not fit in the standard Report on Compliance template, including details on compensating controls.

The Report on Compliance must include a section on 'controls in place' to verify compliance. Your organization cannot be compliant if there are open items, or items to be addressed at a future date. Validation of compliance is all or nothing, so you must address all issues to be compliant.

Your acquirer or card brand may request additional responses to reports submitted for PCI compliance. In this event, you must provide satisfactory responses in order to receive official certification of compliance with PCI DSS.

Compliance with PCI really is more than a one-time annual event. Certification is actually for a mere snapshot in time, and doesn't guarantee you'll be in technical compliance weeks or months after that event occurs. You must continuously follow the process of assessment, remediation, and reporting to ensure the ongoing safety of cardholder data. Be safe, not sorry!

Part V

Ten Best Practices for PCI Compliance

In This Part

- Understanding what's required for PCI compliance
- Following steps to implement controls and processes for compliance
- Making PCI compliance a continuous, ongoing process

This chapter is a handy ten-point checklist of best practices for complying with the PCI Data Security Standard to protect cardholder data. Compliance is something every merchant must do if it stores, processes or transmits payment cardholder data. In this Retail Age of Universal Plastic, virtually no merchant is immune from meeting PCI compliance.

Read This Book

In case you're reading this chapter first, be advised that (in our humble opinion) there's no quicker way for a merchant to get the gist of PCI than to read *PCI Compliance For Dummies*. This book describes the major requirements and summarizes the myriad of sections and sub-sections of details you find in the PCI Data Security Standard. Start here – you won't be sorry!

Know the Risks You Face in Protecting Cardholder Data

Before a merchant can protect cardholder data, you must first understand the nature of risks that threaten cardholder data throughout the process of accepting a payment card and

processing the transaction. Some risks are your direct responsibility. The PCI Data Security standard describes the merchant requirements for meeting this responsibility.

Build and Maintain a Secure Network for Cardholder Data

The network is the glue connecting payment card terminals, processing systems, and retail commerce in general. By exploiting network vulnerabilities, a criminal can access cardholder data much more easily than when thieves had to gain physical access to your building and systems. Merchants must use controls to protect the network, including a firewall configuration. You also need to change vendor-supplied default passwords and other security settings.

Protect Cardholder Data That's Stored or Transmitted

Merchants need to use one or more technical methods of protecting cardholder data, such as encryption, truncation, masking and hashing. These methods make cardholder data unreadable to unauthorized people. Even if a thief manages to smash through security controls and obtain cardholder data, the information has no value because the thief is unable to read and use it. You must protect cardholder data that's stored or transmitted over open, public networks.

Maintain a Vulnerability Management Program

Vulnerability management (VM) is a process that every merchant needs to use to avoid exploitation of weaknesses in your card payment infrastructure. New vulnerabilities appear every day due to flaws in software, faulty configuration of applications and IT gear, and good old human error. Whatever their source, vulnerabilities don't go away by themselves.

Their detection, removal, and control require vulnerability management. VM is the regulated, continuous use of specialized security tools and workflow that actively help to eliminate exploitable risks. As part of a comprehensive VM program, you must use and regularly update anti-virus software or programs, and use only secure systems and applications.

Implement Strong Access Control Measures

Access control is your power to permit or deny the use of physical or technical means to access PAN or other cardholder data. You need to ensure that cardholder data can be accessed only by employees with a business need-to-know You also need to enforce policy for logical and physical access to paper-based records and cardholder system hardware.

Regularly Monitor and Test Networks

Your network is one of the most important elements in the cardholder data environment. Physical and wireless networks enable the flow of cardholder data from PIN entry devices and PCs to servers, payment applications, storage media, and onward to the third-party processor or acquiring bank. A vulnerability existing at any point of the network spells trouble if a data thief exploits it for unauthorized access to cardholder data. Merchants must regularly monitor and test all of their networks to find and fix vulnerabilities – before trouble occurs. At a minimum, you must have an Approved Scanning Vendor scan your external network at least once a quarter. Always scan the network right after making a big system change. Use tools to inspect security logs every day.

Maintain an Information Security Policy

A merchant organization needs to govern all PCI security activity with clear security policies. The policies make it easier to create and follow your PCI compliance program. The result of good policies makes it easier and faster for your IT security team to discover vulnerabilities in the cardholder data environment, remediate those security holes, and produce documentation to satisfy requirements for compliance.

Submit Reports for Quarterly Scans and Annual Review

For most merchants, the formal process of PCI compliance consists of submitting the annual Self-Assessment Questionnaire and quarterly network scan reports generated by an Approved Scanning Vendor. Obviously, merchants want to comply with the spirit of PCI, which is to protect cardholder data. But you also want to comply with the letter of law – verifying that you've passed all requirements of the standard. Getting that certification is essential to avoid penalties by the card brands, such as losing the right to accept their payment card. Ouch!

Make PCI Compliance a Continuous, Ongoing Process

PCI compliance is more than a one-time annual event. Annual certification doesn't guarantee that you'll be in technical compliance weeks or months after certification. You must continuously follow the process of assessment, remediation, and reporting to ensure the ongoing safety of cardholder data. The results are well worth it.

Qualys: The Leader of On-Demand PCI Scanning and Compliance

Qualys is a PCI Approved Scanning Vendor and provider of QualysGuard PCI – the de facto standard on-demand solution for PCI scanning and compliance. QualysGuard PCI is used by more than half of all ASVs and Qualified Security Assessors to scan their clients' networks for PCI, and for PCI self-scanning by thousands of merchant organizations worldwide. QualysGuard PCI is easy to use. It enables you to automatically scan your network, completes a Self-Assessment Questionnaire, and submits the document to your acquirer or card brand for certification of compliance. It lets you do unlimited PCI scanning – both for PCI compliance and to help identify and remediate vulnerabilities as soon as they appear in the network. QualysGuard PCI is a turnkey solution that will help you protect cardholder data and comply with the PCI Data Security Standard.

QualysGuard Awards

QualysGuard is overwhelmingly recognized as the leader in its space. QualysGuard has won awards ranging from Best Vulnerability Management Solution, Best Security Product, Best Security Company, Best Network Protection Service and much more!

PCI Compliance for merchants needn't be scary!

Successfully learn how to comply with PCI and protect cardholder data!

Complying with the PCI Data Security Standard may seem like a daunting task. This book is a quick guide to understanding how to protect cardholder data and comply with requirements of PCI – from surveying the standard's requirements to detailing steps for verifying compliance. This book also tells you about the leading PCI scanning and compliance solution – QualysGuard PCI.

Discover

- *What PCI is all about*
- *The twelve requirements of the PCI standard*
- *How to comply with PCI*
- *Ten best practices for PCI compliance*

THE DUMMIES WAY®

- *Explanations in plain English*
- *'Get in, get out' information*
- *Icons and other navigational aids*
- *A dash of humour and fun*

Get smart! @www.dummies.com

An electronic version of this book is available at www.qualys.com/pcifordummies.

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Browse our free articles*

ISBN: 978-0-470-74452-9
Not for resale

For Dummies®
A Branded Imprint of
WILEY