

A NetClarity, Inc. White Paper



NetClarity, Inc.
54 Middlesex Turnpike, Building C
Bedford, Massachusetts, USA 01730
Tel: 781-276-4555
Fax: 781-276-1569
<http://www.netclarity.net>

Self Assessment for the Payment Card Industry (PCI) Standard

*By Gary S. Miliefsky, CISSP®
Founder & CTO*

2007 Edition

CONTENTS

INTRODUCTION	3
OVERVIEW OF PCI.....	4
DO YOU SPEAK CVE?	6
WHAT IS ISO27001/17799®?	7
REQUIREMENTS OF PCI	8
CVE® AND ISO27001/17799® AUDITING FOR PCI	9
DETECT AND TRACK ASSETS	9
AUDIT YOUR NETWORK FOR CVEs	9
LOCK THE DOORS AGAINST CVE EXPLOITS.....	9
CLEANUP YOUR CVEs.....	9
AUDIT YOURSELF UNDER THE ISO27001/17799® STANDARD	10
PLAN OF ACTION FOR COMPLIANCE	11
ASSESSMENT ON COMPLIANCE	11
REPORTING ON COMPLIANCE	11
SUMMARY	12
CREDITS:.....	12
ABOUT THE AUTHOR:	12

INTRODUCTION

Visa, MasterCard and other payment card companies have collaborated to create a single set of worldwide requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection across the entire industry.

The PCI Data Security Standard aligns Visa's Account Information Security (AIS) program, also known as Cardholder Information Security Program (CISP) in the U.S., and MasterCards' Site Data Protection (SDP) program, streamlining requirements, compliance criteria and validation processes. It also addresses merchants' and acquirers' concerns about having to meet more than one set of standards to accomplish a single goal.

Failure to comply with these regulations could result in fines to merchants and card processors which reach as high as \$500,000 per incident for those out of compliance at the time of the breach. Each retailer, e-commerce company, ISP hosting e-commerce transactions and card processing company needs to be aware which level it is classified as to achieve compliance.

You have two options to comply - self-assess or use an external auditing company that has been approved by the PCI (SDP) program. Self-assessment forms are available online, a sample of which has been added to the end of this white paper for your convenience.

However to maintain currency with the program, please visit:

http://www.usa.Visa.com/business/accepting_Visa/ops_risk_management/cisp.html

<https://sdp.mastercardintl.com/>

The other option, hiring IT Auditors and IT Consultants, may help you shift some of the risk associated with PCI compliance, however, ultimately, you are still responsible for due care and due diligence in protecting the data and the network. This option is very expensive. Please make sure if you chose this option to find a firm you trust - ask for references, check those references and make sure these organizations have been approved by VISA or MasterCard.

There is a consortium that has formed around the PCI model. For more information, please visit:

<https://www.pcisecuritystandards.org>

OVERVIEW OF PCI

PCI is directed to all entities that store, process, or transmit credit cardholder data. Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. The account number is the critical component that makes PCI applicable. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data, however, PCI applies even if the only data stored, processed, or transmitted is account numbers.

The PCI program is broken down into two areas of audit procedures - assessment and reporting on compliance. In summary:

ASSESSMENT ON COMPLIANCE

- Audit all physical and network connections for proper access control
- Audit all data repositories and IP-based POS terminals for proper access control

REPORTING ON COMPLIANCE

- Contact Information
- Executive Summary
- Description of Scope of Work and Approach Taken
- Quarterly CVE® Scan Results
- Findings and Observations

If a requirement is not, or cannot, be met exactly as stated, compensating controls can be considered as alternatives to requirements defined in PCI. Compensating controls should meet the intention and rigor of the original PCI requirement, and should also be examined by the assessor as part of the regular PCI audit. Compensating controls should be above and beyond other PCI requirements - it is not a compensating control to simply be in compliance with other PCI requirements.

Stored cardholder data should be rendered unreadable according to requirement 3 of the PCI Security Audit Procedures document. If encryption, truncation, or another comparable approach cannot be used, encryption options should continue to be investigated as the technology is rapidly evolving. In the interim, while encryption solutions are being investigated, stored data must be strongly protected by compensating controls. These compensating controls should be considered as part of the compliance validation process.

An example of compensating controls for encryption of stored data is complex network segmentation that may include the following:

Internal firewalls that specifically protect the database

TCP wrappers or firewall on the database to specifically limit who can connect to the database

Separation of the corporate internal network on a different network segment from production, firewalled away from database servers.

Members, merchants, and service providers should be in the process of positioning themselves to deal only with PCI-compliant service providers. If there are service providers handling cardholder data on an entity's behalf, the entity must ensure that contracts with these service providers specifically include PCI compliance as a condition of business. A list of compliant service providers can be found on the PCI and SDP websites.

Lack of full compliance will prevent an entity from being considered PCI compliant, however, Visa and MasterCard both encourage entities to complete the initial review, develop a remediation plan, complete items on the remediation plan, and revalidate compliance of those outstanding items. For service providers, a report on compliance demonstrating full compliance must be provided to Visa or MasterCard prior to inclusion on the list of compliant service providers. Currently, there is not a comparable list for merchants.

Protecting your data and network requires intimate knowledge of two internationally accepted security models - the first is MITRE's CVE® program and the second is the ISO27001/17799® standard. CVE® will help you self-assess and document the weak spots in your network assets - your common vulnerabilities and exposures.

By knowing your weak spots, you can begin a process of due care and due diligence to harden your network against attack. ISO27001/17799® will help you self-assess your corporate security policies against the best practices model of the ISO, which is all-inclusive and comprehensive against what PCI and SDP requires.

DO YOU SPEAK CVE?

The most important information security question you need to answer is **Do You Speak CVE?** If you do not, then no matter how much you spend on INFOSEC countermeasures, you'll never fully understand why you are experiencing downtime and successful hacker attacks. Not to mention the regulatory compliance risk you face.

Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. Using a common name makes it easier to share data across separate databases and tools that until now were not easily integrated. This makes CVE the key to information sharing. If a report from one of your security tools incorporates CVE names, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

CVE – An Industry Standard funded by the Department of Homeland Security – Operated by MITRE.

CVE is:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Accessible for review or download from the Internet
- Industry-endorsed via the CVE Editorial Board

Some CVEs are currently Candidates (CANs) – keep an eye out on both CVEs and CANidate CVEs.

Example CANDidate CVE:

CAN-2003-0352 (under review)

Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message.

What exploited this CVE? Blaster, Msblast, LovSAN and the Nachi and Welchia worms causing massive downtime and financial losses.

WHAT IS ISO27001/17799®?

The ISO27001/17799® model for information security comes from the International Organization for Standardization (ISO).

ISO is a network of national standards institutes from 146 countries working in partnership with international organizations, governments, industry, business and consumer representatives. ISO also serves as a bridge between public and private sectors. You can learn more about ISO at <http://www.iso.org>.

The ISO27001/17799® standard contains ten sections:

1. **Security Policy** – To provide management direction and support for information security
2. **Organizational Security** – To manage information security within the organization
3. **Asset Classification and Control** – To maintain proper classification and protection of organizational assets
4. **Personnel Security** – To reduce the risk of human error, theft, fraud or misuse of your company or organization
5. **Physical and Environmental Security** – To prevent unauthorized access, damage and interference to business premises and information
6. **Communications and Operations Management** – To ensure the correct and secure operations of information processing
7. **Access Control** – To control access to information
8. **System Development and Maintenance** – To ensure security is built into information systems development and maintenance processes
9. **Business Continuity Management** – To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters otherwise known as BCP/DRP
10. **Compliance** – To avoid breaches of any criminal and civil law, statutory, regulatory or contractual within your business model and government guidelines

REQUIREMENTS OF PCI

Visa and MasterCard require you to take best practices security measures to ensure protection of credit card holder data, all related transactions and information storage. To do so, you must build and maintain a secure network, a vulnerability management program, implement strong access control measures, regularly monitor and test networks and maintain an information security policy as follows:

Build & Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect Stored Data
- Encrypt transmission of cardholder and sensitive Information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for employees and contractors

CVE® AND ISO27001/17799® AUDITING FOR PCI

By protecting yourself against CVE® exploiters, you will be taking proactive steps of due care and due diligence for PCI. There are four key things you can do to protect yourself against CVE® exploiters:

- 1. Detect and Track Assets**
- 2. Audit your Network for CVEs**
- 3. Lock The Doors against CVE Exploits**
- 4. Cleanup your CVEs**

DETECT AND TRACK ASSETS

Do you have policies and systems in place to track all of your network-based assets? Do you allow laptops in and out of the office? Are laptops a company asset or a personal computer that can be used at home? Do you require firewall, antivirus, antispymware and patches to be installed on each host and up to date? What about wireless routers and ad-hoc wireless LANs – have you sniffed the airwaves and port connections to see if there are any new wireless devices or servers connected to your network? Answering these questions is critical in the protection of these assets against CVE exploiters.

AUDIT YOUR NETWORK FOR CVEs

Find a tool you like. Google [Laptop Auditor](#) or [Security Auditor](#) or use similar keywords and you'll find companies and products in this marketplace. Do an evaluation of open source versus commercial products. If you built your firewall from scratch – go for open source, otherwise find a company you can work with and trust. Make sure to pick a tool that doesn't take any assets offline and scans and reports on CVEs.

LOCK THE DOORS AGAINST CVE EXPLOITS

Your firewall is your best countermeasure. Make sure to review logs – look for suspicious traffic. Also make sure you setup the VPN interface properly and know who's using it and if they are coming in through a secure tunnel on an insecure or sick' computer. By reconfiguring your rules table around CVE Exploits, you might be one step ahead of the hackers. For example, why not block ports for all inbound/outbound traffic that you don't use – 445 was exploited by MSBlast and Sasser. Do you need to keep this port open at the firewall? Look at the computers that have CVEs – how long to fix and what port is it on? Update your rules table until it is fixed. Don't trust all patches. Reinspect for same or new CVEs and the affected ports and services. Keep repeating this process, daily.

CLEANUP YOUR CVEs

Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change and no CVE to exploit. Some CVEs can be patched while

others require intelligent reconfiguration.
Cleanup your CVEs on the most important systems and highest risk of attack. Keep repeating this process, daily.

AUDIT YOURSELF UNDER THE ISO27001/17799® STANDARD

In addition, you should build a Corporate Security Policy that complies with the ISO27001/17799® standard. Here are some of the key areas in the ISO27001/17799® standard which you may use to correlate with the PCI standard:

Build & Maintain a Secure Network – SECTION 7 OF ISO27001/17799®

- Install and maintain a firewall configuration to protect data
- Do not use vendor supplied defaults for system passwords and other security parameters

Protect Cardholder Data – SECTION 10 OF ISO27001/17799®

- Protect Stored Data
- Encrypt transmission of cardholder and sensitive Information across public networks

Maintain a Vulnerability Management Program – SECTION 8 OF ISO27001/17799®

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures – SECTION 8 OF ISO27001/17799®

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks – SECTION 6 OF ISO27001/17799®

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy – SECTION 1 OF ISO27001/17799®

- Maintain a policy that addresses information security for employees and contractors

PLAN OF ACTION FOR COMPLIANCE

ASSESSMENT ON COMPLIANCE

First, audit yourself against the ISO27001/17799® standard and develop an ISO17799® compliant Corporate Security policy. You can do this by using NetClarity's Auditor Enterprise™ appliance from the Advanced Policy Auditing and Building tools menu item or you can hire a PCI or SDP approved IT Consulting firm.

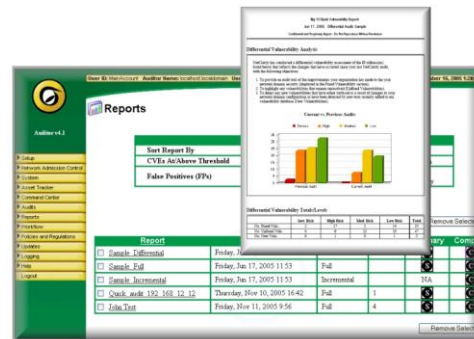
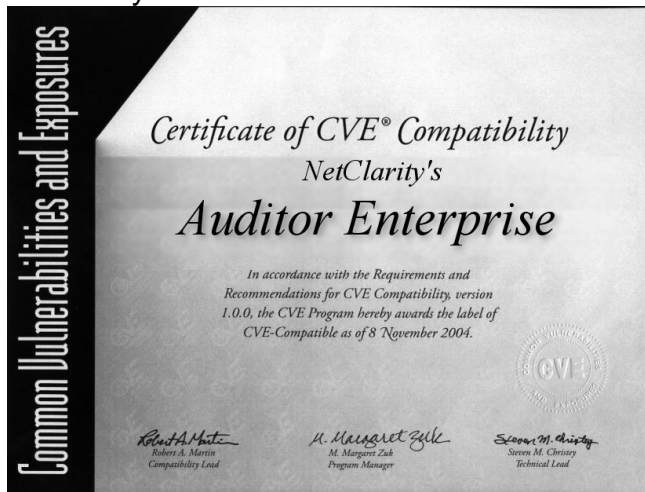
REPORTING ON COMPLIANCE

Second, generate a CVE® analysis of all the important assets on your network. Begin a workflow and remediation process to harden your network and remove your CVE®s. Then, generate a CVE® gap analysis against the PCI standard. Again, this can be done very rapidly using NetClarity's Auditor Enterprise™ or by hiring a PCI or SDP approved IT Consulting firm.

Then, use the PCI Security Self-Assessment Questionnaire and organize the following information in a package you will send into Visa or MasterCard:

- Contact Information
- Executive Summary
- Description of Scope of Work and Approach Taken
- Quarterly CVE® Scan Results
- Findings and Observations

When choosing to do it yourself using CVE® approved self-assessment tools, make sure they are certified by MITRE. Here's an example of the type of certification that should be available to you from a CVE® tool vendor, such as NetClarity:



SUMMARY

Visa, MasterCard and other payment card companies have collaborated to create a single set of worldwide requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection across the entire industry. The PCI Data Security Standard aligns Visa's Account Information Security (AIS) program, also known as Cardholder Information Security Program (CISP) in the U.S., and MasterCards' Site Data Protection (SDP) program, streamlining requirements, compliance criteria and validation processes. It also addresses merchants' and acquirers' concerns about having to meet more than one set of standards to accomplish a single goal.

Failure to comply with these regulations could result in fines to merchants and card processors which reach as high as \$500,000 per incident for those out of compliance at the time of the breach. Keep an eye on these two web sites to keep up to date with the PCI and SDP standards:

http://www.usa.Visa.com/business/accepting_Visa/ops_risk_management/cisp.html

<https://sdp.mastercardintl.com/>

You have two options to comply - self-assess or use an external auditing company that has been approved by the PCI or SDP program.

NetClarity provides a turnkey solution to help you self-assess - Auditor EnterpriseTM. For more information on these appliances, please visit:

www.netclarity.net

CREDITS:

Thanks to numerous NetClarity customers for their time in reviewing this document and suggestions. Many thanks to the MITRE CVE team, <http://cve.mitre.org>, for their work in creating and standardizing CVEs.

CVE® and the CVE logo are registered trademarks of The MITRE Corporation. Use of the Common Vulnerabilities and Exposures List and the associated references from MITRE are subject to the Terms of Use.

For more information, please email cve@mitre.org

CVE® is sponsored by U.S. Department of Homeland Security. For more information, please visit <http://www.us-cert.gov>



Portions excerpted from VISA PCI and MasterCard SDP under the fair use guidelines of U.S. Copyright Law.

ABOUT THE AUTHOR:



Gary S. Miliefsky, CISSP®

Founder & CTO
NetClarity, Inc.

Gary Miliefsky has 20+ years experience as an entrepreneur, computer scientist and trained security professional. He has been CEO and/or CTO of 3 start-up ventures. Mr. Miliefsky is a founding member of the Department of Homeland Security, <http://www.usdhs.gov/>. He currently serves as an advisor to MITRE Corporation at <http://oval.mitre.org/> and is a member of the New England Information Security Group's Board of Directors, found at <http://www.neisg.org/>. He received his undergraduate degree from UMASS Lowell in Computer Science and subsequently earned certification as a CISSP®. Mr. Miliefsky holds six e-commerce patents and has seven network security patents pending, including one about Proactive Network Security Using RSS. He maintains a Blog about IT Security Tips, Trends and News at <http://netclarity.blogspot.com>.

COPYRIGHT NOTICE:

All rights reserved. Printed in the United States of America. No part of this Whitepaper may be reproduced in any form and by any means without prior written permission of NetClarity, Inc. Making copies for any other use than backup purposes is a violation of US and International copyright laws. Copyright © 2006, NetClarity, Inc.

CONTACT INFORMATION:

Feel free to visit Gary online at <http://www.netclarity.net>. If you have any questions about this paper, please send an email to support@netclarity.net.

NetClarity, Inc.
54 Middlesex Turnpike, Building C
Bedford, Massachusetts, USA 01730
Tel: 781-276-4555 Fax: 781-276-1569 SKYPE: netclarity Web: <http://www.netclarity.net/>





Payment Card Industry Self-Assessment Questionnaire

How to Complete the Questionnaire

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard. For any questions where N/A is marked, a brief explanation should be attached.

Questionnaire Reporting

The following must be included with the self-assessment questionnaire and system perimeter scan results:

Organization Information

CORPORATE NAME:		DBA(S):	
CONTACT NAME:		TITLE:	
PHONE:		E-MAIL:	
APPROXIMATE NUMBER OF TRANSACTIONS/ACCOUNTS HANDLED PER YEAR:			

Please include a brief description of your business.

Please explain your business' role in the payment flow. How and in what capacity does your business store, process and/or transmit cardholder data?

List all Third Party Service Providers

Processor:		Gateway:	
Web Hosting		Shopping Cart:	
Co-Location:		Other:	

List Point of Sale (POS) software/hardware in use:



Rating the Assessment

After completing each section of the assessment, users should fill in the rating boxes as follows:

IN EACH SECTION IF...	THEN, THE SECTION RATING IS ...
ALL questions are answered with yes or N/A	Green - The merchant or service provider is compliant with the self-assessment portion of the PCI Data Security Standard. <i>Note: If "N/A" is marked, attach a brief explanation.</i>
ANY questions are answered with no	Red – The merchant or service provider is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

Section 1:	Green Red	Section 4:	Green Red
Section 2:	Green Red	Section 5:	Green Red
Section 3:	Green Red	Section 6:	Green Red
Overall Rating:		Green	Red

Glossary

A glossary of terms can be found on the CISP website:

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_GlossaryofTerms.pdf

Build and Maintain a Secure Network

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

DESCRIPTION		RESPONSE		
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.2	If wireless technology is used, is the access to the network limited to authorized devices?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.3	Do changes to the firewall need authorization and are the changes logged?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

Build and Maintain a Secure Network

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

	DESCRIPTION	RESPONSE		
2.1	Are vendor default security settings changed on production systems before taking the system into production?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
2.6	Are secure, encrypted communications used for remote administration of production systems and applications?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Protect Cardholder Data

Requirement 3: Protect stored data

DESCRIPTION		RESPONSE	
3.1	Is sensitive cardholder data securely disposed of when no longer needed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3.4	Are all but the last four digits of the account number masked when displaying cardholder data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3.6	Are account numbers sanitized before being logged in the audit log?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

DESCRIPTION		RESPONSE		
4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.3	If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.5	Is encryption used in the transmission of account numbers via e-mail?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

	DESCRIPTION	RESPONSE
5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Requirement 6: Develop and maintain secure systems and applications

	DESCRIPTION	RESPONSE
6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.3	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.4	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.7	Is sensitive cardholder data stored in cookies secured or encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Implement Strong Access Control Measures

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

	DESCRIPTION	RESPONSE	
7.1	Is access to payment card account numbers restricted for users on a need-to-know basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

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

	DESCRIPTION	RESPONSE		
8.1	Are all users required to authenticate using, at a minimum, a unique username and password?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.3	Are all passwords on network devices and systems encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.4	When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer users?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.9	Are non-consumer users required to change their passwords on a pre-defined regular basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

DESCRIPTION		RESPONSE		
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

Regularly Monitor and Test Networks

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

	DESCRIPTION	RESPONSE
10.1	Is all access to cardholder data, including root/administration access, logged?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Requirement 11: Regularly test security systems and processes

	DESCRIPTION	RESPONSE
11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.3	Is an intrusion detection or intrusion prevention system used on the network?	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Regularly Monitor and Test Networks

Requirement 12: Maintain a policy that addresses information security

	DESCRIPTION	RESPONSE	
12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.3	Are information security policies reviewed at least once a year and updated as needed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.4	Have the roles and responsibilities for information security been clearly defined within the company?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.5	Is there an up-to-date information security awareness and training program in place for all system users?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.7	Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.10	Are security incidents reported to the person responsible for security investigation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise?	<input type="checkbox"/> Yes	<input type="checkbox"/> No