



PCI Compliance
673-401 Woodland Square Loop SE, Lacey, WA 98503 • Phone: 800.687.8505
Fax: 1.866.371.1521 • Email: PCI@FrontStreamPayments.com

Attention: PCI Compliance

Please return this Cover Letter with your Self Assessment Questionnaire (SAQ) to FrontStream Payments via fax, mail or email. To ensure accuracy of the information we have on file, please fill in the following information as well.

If you have any questions please contact our PCI Compliance Department at 800.687.8505 or PCI@FrontStreamPayments.com

Business Legal Name:	Business DBA:
Merchant ID:	PCI Contact Person:
Phone:	Email:
Fax:	Best time/method to contact:

Please note that email or fax may be utilized for SAQ and/or scan renewal notices.

Please provide the following details if you have received your compliance certificate through a source other than FrontStream Payments. If applicable please provide PCI Approved Scanning Vendor (ASV) information.

SAQ Assessment Source And date of Compliance	
PCI Approved Scanning Vendor (ASV), Scan Date and Result:	

Notes: (any questions or comments you might have)

--

Please return your signed SAQ and/or compliance certificate to:

Fax: (866) 371-1521
Email: PCI@FrontStreamPayments.com
Mail: FrontStream Payments
Attn: PCI Compliance
673-401 Woodland Square Loop SE
Lacey, WA 98503

FrontStream Payments | 673 Woodland Square Loop SE, Suite 401 | Lacey, WA 98503
800.687.8505 (Toll Free) / 360.357.1400



**Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire D
and Attestation of Compliance**

**All other SAQ-Eligible Merchants and Service
Providers**

Version 2.0

October 2010

Document Changes

Date	Version	Description
October 1, 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 28, 2010	2.0	To align content with new PCI DSS v2.0 requirements and testing procedures.

Table of Contents

Document Changes	i
PCI Data Security Standard: Related Documents	iii
Before You Begin	iv
Completing the Self-Assessment Questionnaire	iv
PCI DSS Compliance – Completion Steps	iv
Guidance for Non-Applicability of Certain, Specific Requirements	v
Attestation of Compliance, SAQ D—Merchant Version	1
Attestation of Compliance, SAQ D—Service Provider Version	1
Self-Assessment Questionnaire D	1
Build and Maintain a Secure Network	1
<i>Requirement 1: Install and maintain a firewall configuration to protect data</i>	<i>1</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</i>	<i>4</i>
Protect Cardholder Data	6
<i>Requirement 3: Protect stored cardholder data</i>	<i>6</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks</i>	<i>10</i>
Maintain a Vulnerability Management Program	11
<i>Requirement 5: Use and regularly update anti-virus software or programs</i>	<i>11</i>
<i>Requirement 6: Develop and maintain secure systems and applications</i>	<i>11</i>
Implement Strong Access Control Measures	15
<i>Requirement 7: Restrict access to cardholder data by business need to know</i>	<i>15</i>
<i>Requirement 8: Assign a unique ID to each person with computer access</i>	<i>16</i>
<i>Requirement 9: Restrict physical access to cardholder data</i>	<i>19</i>
Regularly Monitor and Test Networks	22
<i>Requirement 10: Track and monitor all access to network resources and cardholder data</i> ..	<i>22</i>
<i>Requirement 11: Regularly test security systems and processes</i>	<i>24</i>
Maintain an Information Security Policy	27
<i>Requirement 12: Maintain a policy that addresses information security for all personnel</i>	<i>27</i>
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers ..	31
.....	
<i>Requirement A.1: Shared hosting providers must protect cardholder data environment</i>	<i>31</i>
Appendix B: Compensating Controls	33
Appendix C: Compensating Controls Worksheet	34
Compensating Controls Worksheet—Completed Example	35
Appendix D: Explanation of Non-Applicability	36

PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard (PCI DSS) and the PCI DSS SAQ.

Document	Audience
<i>PCI Data Security Standard: Requirements and Security Assessment Procedures</i>	All merchants and service providers
<i>Navigating PCI DSS: Understanding the Intent of the Requirements</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Guidelines and Instructions</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Eligible merchants and service providers ¹
<i>PCI Data Security Standard and Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms</i>	All merchants and service providers

¹ To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, “Selecting the SAQ and Attestation That Best Apply to Your Organization.”

Before You Begin

Completing the Self-Assessment Questionnaire

SAQ D has been developed for all SAQ-eligible service providers and for all merchants not meeting the descriptions of SAQ types A through C as described briefly in the table below and fully in *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*.

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants.</i>
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants (not included in descriptions for SAQs A through C above) and all service providers defined by a payment brand as eligible to complete an SAQ.

SAQ D applies to SAQ-eligible merchants not meeting the criteria for SAQ types A through C, above and all service providers defined by a payment brand as being SAQ-eligible. SAQ D service providers and merchants validate compliance by completing SAQ D and the associated Attestation of Compliance. While many of the organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. See the guidance below for information about the exclusion of wireless technology and certain other, specific requirements.

Each section of this questionnaire focuses on a specific area of security, based on the requirements in the PCI DSS.

PCI DSS Compliance – Completion Steps

1. Assess your environment for compliance with the PCI DSS.
2. Complete the Self-Assessment Questionnaire (SAQ D) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
3. Complete a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.
4. Complete the Attestation of Compliance in its entirety.
5. Submit the SAQ, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to your acquirer (for merchants) or to the payment brand or other requester (for service providers).

Guidance for Non-Applicability of Certain, Specific Requirements

Exclusion: If you are required to answer SAQ D to validate your PCI DSS compliance, the following exceptions may be considered. See “Non-Applicability” below for the appropriate SAQ response.

- The questions specific to wireless only need to be answered if wireless is present anywhere in your network (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Note that Requirement 11.1 (use of process to identify unauthorized wireless access points) must still be answered even if wireless is not in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- The questions specific to custom applications and code (Requirements 6.3 and 6.5) only need to be answered if your organization develops its own custom applications.
- The questions for Requirements 9.1 through 9.4 only need to be answered for facilities with “sensitive areas” as defined here. “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data.

Non-Applicability: These and any other requirements deemed not applicable to your environment must be indicated with “N/A” in the “Special” column of the SAQ. Accordingly, complete the “Explanation of Non-Applicability” worksheet in Appendix D for each “N/A” entry.

Attestation of Compliance, SAQ D—Merchant Version

Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant’s compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at PCI DSS Compliance – Completion Steps in this document.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:		DBA(s):	
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

Part 2 Type of merchant business (check all that apply):

- Retailer Telecommunication Grocery and Supermarkets
 Petroleum E-Commerce Mail/Telephone-Order
 Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2a. Relationships

- Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? Yes No
- Does your company have a relationship with more than one acquirer? Yes No

Part 2b. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

Please provide the following information regarding the Payment Applications your organization uses:

<u>Payment Application in Use</u>	<u>Version Number</u>	<u>Last Validated according to PABP/PA-DSS</u>

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated (*completion date*), (*Merchant Company Name*) asserts the following compliance status (check one):

- Compliant:** All sections of the PCI SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; **and** a passing scan has been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Merchant Company Name*) has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered "yes," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Merchant Company Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Merchant confirms:

- PCI DSS Self-Assessment Questionnaire D, Version (*version of SAQ*), was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Merchant Acknowledgement

<i>Signature of Merchant Executive Officer</i> ↑	<i>Date</i> ↑
<i>Merchant Executive Officer Name</i> ↑	<i>Title</i> ↑
<i>Merchant Company Represented</i> ↑	

² Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Use and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	

Attestation of Compliance, SAQ D—Service Provider Version

Instructions for Submission

The service provider must complete this Attestation of Compliance as a declaration of the service provider's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:		DBA(s):	
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	
Lead QSA Contact Name:	
Title:	
Telephone:	
E-mail:	
Business Address:	
City:	
State/Province:	
Country:	
Zip:	
URL:	

Part 2. PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

<input type="checkbox"/> 3-D Secure Hosting Provider	<input type="checkbox"/> Hosting Provider – Hardware	<input type="checkbox"/> Payment Processing – ATM
<input type="checkbox"/> Account Management	<input type="checkbox"/> Hosting Provider – Web	<input type="checkbox"/> Payment Processing – MOTO
<input type="checkbox"/> Authorization	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Payment Processing – Internet
<input type="checkbox"/> Back Office Services	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Payment Processing – POS
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Managed Services	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Records Management
<input type="checkbox"/> Data Preparation	<input type="checkbox"/> Network Provider/Transmitter	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Fraud and Chargeback Services	<input type="checkbox"/> Payment Gateway/Switch	
<input type="checkbox"/> Others (please specify):		

List facilities and locations included in PCI DSS review:

Part 2b. If any services listed are provided by the service provider but *WERE NOT INCLUDED* in the Scope of the PCI DSS Assessment, please check them below:

- | | | |
|--|---|--|
| <input type="checkbox"/> 3-D Secure Hosting Provider | <input type="checkbox"/> Hosting Provider – Hardware | <input type="checkbox"/> Payment Processing – ATM |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Hosting Provider – Web | <input type="checkbox"/> Payment Processing – MOTO |
| <input type="checkbox"/> Authorization | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Payment Processing – Internet |
| <input type="checkbox"/> Back Office Services | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Payment Processing – POS |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Managed Services | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Data Preparation | <input type="checkbox"/> Network Provider/Transmitter | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Fraud and Chargeback Services | <input type="checkbox"/> Payment Gateway/Switch | |
| <input type="checkbox"/> Others (please specify): | | |

Part 2c. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, Yes No etc.)?

Part 2d. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

<u>Payment Application in Use</u>	<u>Version Number</u>	<u>Last Validated according to PABP/PA-DSS</u>

Please provide the following information regarding the Payment Applications your organization uses:

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated (*completion date of SAQ*), (*Service Provider Company Name*) asserts the following compliance status (check one):

- Compliant:** All sections of the PCI SAQ are complete, and all questions answered “yes”, resulting in an overall **COMPLIANT** rating; **and** a passing scan has been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Service Provider Company Name*) has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered “no”, resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Service Provider Company Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Service Provider confirms:

<input type="checkbox"/>	Self-Assessment Questionnaire D, Version (<i>insert version number</i>), was completed according to the instructions therein.
<input type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
<input type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
<input type="checkbox"/>	No evidence of magnetic stripe (i.e., track) data ⁵ , CAV2, CVC2, CID, or CVV2 data ⁶ , or PIN data ⁷ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Service Provider Acknowledgement

<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date</i> ↑
<i>Service Provider Executive Officer Name</i> ↑	<i>Title</i> ↑
<i>Service Provider Company Represented</i> ↑	

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate “Compliance Status” for each requirement. If you answer “NO” to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

⁵ Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

⁶ The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

⁷ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Use and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	

Self-Assessment Questionnaire D

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Date of Completion:

Build and Maintain a Secure Network

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

PCI DSS Question		Response:	Yes	No	Special*
1.1	Are firewall and router configuration standards established to include the following:				
1.1.1	Is there a formal process for approving and testing all external network connections and changes to the firewall and router configurations?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	(a) Is there a current network diagram (for example, one that shows cardholder data flows over the network) that documents all connections to cardholder data, including any wireless networks?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the diagram kept current?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	(a) Do configuration standards include requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the current network diagram consistent with the firewall configuration standards?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Do firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	(a) Do firewall and router configuration standards include a documented list of services, protocols and ports necessary for business (for example, hypertext transfer protocol (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols).		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are all allowed insecure services, protocols, and ports necessary, and are security features documented and implemented for each?		<input type="checkbox"/>	<input type="checkbox"/>	
	<i>Note: Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.</i>				

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:		Yes	No	Special*
1.1.6	(a) Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Are firewall and router rule sets reviewed at least every six months?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows: <i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>					
1.2.1	(a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment, and are the restrictions documented?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.2	Are router configuration files secure and synchronized?	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.3	Are perimeter firewalls installed between any wireless networks and the cardholder data environment, and are these firewalls configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment, as follows:					
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.3	Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.4	Are internal addresses prohibited from passing from the Internet into the DMZ?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.5	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?	<input type="checkbox"/>	<input type="checkbox"/>			
1.3.7	Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?	<input type="checkbox"/>	<input type="checkbox"/>			

PCI DSS Question		Response:		<u>Yes</u>	<u>No</u>	<u>Special</u> *
1.3.8	(a) Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet? Note: <i>Methods to obscure IP addressing may include, but are not limited to:</i> <ul style="list-style-type: none"> • <i>Network Address Translation (NAT)</i> • <i>Placing servers containing cardholder data behind proxy servers/firewalls or content caches,</i> • <i>Removal or filtering of route advertisements for private networks that employ registered addressing,</i> • <i>Internal use of RFC1918 address space instead of registered addresses.</i> 	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Is any disclosure of private IP addresses and routing information to external entities authorized?	<input type="checkbox"/>	<input type="checkbox"/>			
1.4	(a) Is personal firewall software installed and active on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Is the personal firewall software configured to specific standards, and not alterable by mobile and/or employee-owned computer users?	<input type="checkbox"/>	<input type="checkbox"/>			

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

PCI DSS Question		Response:		Special*
		Yes	No	
2.1	Are vendor-supplied defaults always changed before installing a system on the network? <i>Vendor-supplied defaults Include but are not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are defaults changed as follows:			
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are default SNMP community strings on wireless devices changed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are default passwords/passphrases on access points changed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Are other security-related wireless vendor defaults changed, if applicable?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards? Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are system configuration standards updated as new vulnerability issues are identified, as defined in requirement 6.2?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are system configuration standards applied when new systems are configured?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Do system configuration standards include the following:			
2.2.1	(a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server? (For example, web servers, database servers, and DNS should be implemented on separate servers.)	<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:		Special*
		Yes	No	
	(b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are all enabled insecure services, daemons, or protocols justified, and are security features documented and implemented? <i>(For example, secured technologies such as SSH, S-FTP, SSL, or IPSec VPN are used to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.)</i>	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are common system security parameters settings included in the system configuration standards?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are security parameter settings set appropriately on system components?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	(a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are enabled functions documented and do they support secure configuration?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is only documented functionality present on system components?	<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Is non-console administrative access encrypted as follows: <i>Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</i>			
	(a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	<input type="checkbox"/>	<input type="checkbox"/>	
2.4	If you are a shared hosting provider, are your systems configured to protect each entity's hosted environment and cardholder data? See Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers <i>for specific requirements that must be met.</i>	<input type="checkbox"/>	<input type="checkbox"/>	

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Response:		Special*
		Yes	No	
3.1	Are data retention and disposal policies and procedures implemented as follows:			
3.1.1	(a) Are data retention and disposal policies and procedures implemented and do they include specific requirements for retention of cardholder data as required for business, legal, and/or regulatory purposes? <i>For example, cardholder data needs to be held for X period for Y business reasons.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do policies and procedures include provisions for the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Do policies and procedures include coverage for all storage of cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Do processes and procedures include at least one of the following? <ul style="list-style-type: none"> • A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy • Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy. 	<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Does all stored cardholder data meet the requirements defined in the data retention policy?	<input type="checkbox"/>	<input type="checkbox"/>	
3.2	(a) For issuers and/or companies that support issuing services and store sensitive authentication data, is there is a business justification for the storage of sensitive authentication data, and is that the data is secured?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For all other entities, if sensitive authentication data is received and deleted, are processes in place to securely delete the data to verify that the data is unrecoverable?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):			

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1 The full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance? This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. <i>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i> <ul style="list-style-type: none"> ▪ The cardholder's name, ▪ Primary account number (PAN), ▪ Expiration date, and ▪ Service code <i>To minimize risk, store only these data elements as needed for business.</i>	<input type="checkbox"/>	<input type="checkbox"/>		
3.2.2 The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance?	<input type="checkbox"/>	<input type="checkbox"/>		
3.2.3 The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance?	<input type="checkbox"/>	<input type="checkbox"/>		
3.3 Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)? <i>Notes:</i> <ul style="list-style-type: none"> ▪ This requirement does not apply to employees and other parties with a specific need to see the full PAN; ▪ This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. 	<input type="checkbox"/>	<input type="checkbox"/>		
3.4 Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches? <ul style="list-style-type: none"> ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. <i>Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.</i>	<input type="checkbox"/>	<input type="checkbox"/>		
3.4.1 If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows:				

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
(a) Is logical access to encrypted file systems managed independently of native operating system access control mechanisms (for example, by not using local user account databases)?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Is cardholder data on removable media encrypted wherever stored? Note: <i>If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5 Are any keys used to secure cardholder data protected against disclosure and misuse as follows: Note: <i>This requirement also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.</i>				
3.5.1 Is access to cryptographic keys restricted to the fewest number of custodians necessary?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2 (a) Are keys stored in encrypted format and are key-encrypting keys stored separately from data-encrypting keys?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Are cryptographic keys stored in the fewest possible locations and forms?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6 (a) Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) For service providers only: If keys are shared with customers for transmission or storage of cardholder data, is documentation provided to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with requirements 3.6.1 through 3.6.8 below?		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Are key-management processes and procedures implemented to require the following:				
3.6.1 Do cryptographic key procedures include the generation of strong cryptographic keys?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2 Do cryptographic key procedures include secure cryptographic key distribution?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3 Do cryptographic key procedures include secure cryptographic key storage?		<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question	Response:	Response:		Special*
		Yes	No	
3.6.4	Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	(a) Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do cryptographic key procedures include replacement of known or suspected compromised keys?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes (not used for encryption operations)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Do cryptographic key procedures include split knowledge and dual control of cryptographic keys (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key), for manual clear-text key-management operations? <i>Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys?	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities?	<input type="checkbox"/>	<input type="checkbox"/>	

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

PCI DSS Question		Response:		Special*
		Yes	No	
4.1	<p>(a) Are strong cryptography and security protocols, such as SSL/TLS, SSH or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS include but are not limited to the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are only trusted keys and/or certificates accepted?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are security protocols implemented to use only secure configurations, and not support insecure versions or configurations?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(e) For SSL/TLS implementations:</p> <ul style="list-style-type: none"> Does HTTPS appear as part of the browser Universal Record Locator (URL)? Is cardholder data required only when HTTPS appears in the URL? 	<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	<p>Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?</p> <p>Note: <i>The use of WEP as a security control was prohibited as of 30 June, 2010.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	(a) Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	<input type="checkbox"/>	<input type="checkbox"/>	

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Maintain a Vulnerability Management Program

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

PCI DSS Question		Response:		Yes	No	Special*
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	<input type="checkbox"/>	<input type="checkbox"/>			
5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	<input type="checkbox"/>	<input type="checkbox"/>			
5.2	Is all anti-virus software current, actively running, and generating audit logs as follows:					
	(a) Does the anti-virus policy require updating of anti-virus software and definitions?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Is the master installation of the software enabled for automatic updates and scans?	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Are automatic updates and periodic scans enabled?	<input type="checkbox"/>	<input type="checkbox"/>			
	(d) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	<input type="checkbox"/>	<input type="checkbox"/>			

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Response:		Yes	No	Special*
6.1	(a) Are all system components and software protected from known vulnerabilities by having the latest vendor-supplied security patches installed?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Are critical security patches installed within one month of release?	<input type="checkbox"/>	<input type="checkbox"/>			
	<p>Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.</p>					

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:	Yes	No	Special*
6.2	<p>(a) Is there a process to identify newly discovered security vulnerabilities, including a risk ranking that is assigned to such vulnerabilities? (At minimum, the most critical, highest risk vulnerabilities should be ranked as “High”.)</p> <p>Note: Risk rankings should be based on industry best practices. For example, criteria for ranking ‘High’ risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as “critical”, and/or a vulnerability affecting a critical system component.</p> <p><i>The ranking of vulnerabilities is considered a best practice until June 30, 2012, after which it becomes a requirement.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do processes to identify new security vulnerabilities include using outside sources for security vulnerability information?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Are software development processes based on industry standards and/or best practices?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is information security included throughout the software development life cycle?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Do software development processes ensure the following?				
6.3.1	Are custom application accounts, user IDs, and/or passwords removed before applications become active or are released to customers?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	<p>Are all custom application code changes reviewed (either using manual or automated processes) prior to release to production or customers in order to identify any potential coding vulnerability as follows:</p> <ul style="list-style-type: none"> • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices? • Code reviews ensure code is developed according to secure coding guidelines (per PCI DSS Requirement 6.5)? • Appropriate corrections are implemented prior to release? • Code review results are reviewed and approved by management prior to release? <p>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public-facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</p>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	Are change control processes and procedures followed for all changes to system components to include the following:				

PCI DSS Question		Response:		Special*
		Yes	No	
6.4.1	Are development/test environments separate from the production environment, and is access control in place to enforce the separation?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Are production data (live PANs) not used for testing or development?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Are test data and accounts removed before production systems become active?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5	(a) Are change control procedures for implementing security patches and software modifications documented and require items 6.4.5.1 – 6.4.5.4 below?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the following performed for all changes:			
6.4.5.1	Documentation of impact?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5.2	Documented approval by authorized parties?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5.3	(a) Functionality testing to verify that the change does not adversely impact the security of the system?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For custom code changes, are updates tested for compliance with PCI DSS Requirement 6.5 before being deployed into production?	<input type="checkbox"/>	<input type="checkbox"/>	
6.4.5.4	Are back-out procedures prepared for each change?	<input type="checkbox"/>	<input type="checkbox"/>	
6.5	(a) Are applications developed based on secure coding guidelines? (For example, the <i>Open Web Application Security Project (OWASP) Guide</i> , <i>SANS CWE Top 25</i> , <i>CERT Secure Coding</i> , etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are developers knowledgeable in secure coding techniques?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is prevention of common coding vulnerabilities covered in software development processes to ensure that applications are not vulnerable to, at a minimum the following: <i>Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated, the current best practices must be used for these requirements.</i>			
6.5.1	Injection flaws, particularly SQL injection? (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.) <i>Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Buffer overflow? (Validate buffer boundaries and truncate input strings.)	<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Insecure cryptographic storage? (Prevent cryptographic flaws.)	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:	Yes	No	Special*
6.5.4	Insecure communications? (Properly encrypt all authenticated and sensitive communications.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Improper error handling? (Do not leak information via error messages.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2)? <i>Note: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
For web applications and application interfaces (internal or external), are the following additional vulnerabilities also addressed:					
6.5.7	Cross-site scripting (XSS)? (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Improper Access Control such as insecure direct object references, failure to restrict URL access, and directory traversal? (Properly authenticate users and sanitize input. Do not expose internal object references to users.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Cross-site request forgery (CSRF)? (Do not reply on authorization credentials and tokens automatically submitted by browsers.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.6	For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying <i>either</i> of the following methods? <ul style="list-style-type: none"> ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: <ul style="list-style-type: none"> ○ At least annually ○ After any changes ○ By an organization that specializes in application security ○ That all vulnerabilities are corrected ○ That the application is re-evaluated after the corrections – or – ▪ Installing a web-application layer firewall in front of public-facing web applications to detect and prevent web-based attacks. <p><i>Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	

Implement Strong Access Control Measures

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

PCI DSS Question		Response:		Special*
		Yes	No	
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:			
7.1.1	Are access rights for privileged user IDs restricted to least privileges necessary to perform job responsibilities?	<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Are privileges assigned to individuals based on job classification and function (also called "role-based access control" or RBAC)?	<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Is documented approval by authorized parties required (in writing or electronically) that specifies required privileges?	<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Are access controls implemented via an automated access control system?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2	Is an access control system in place for systems with multiple users to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:			
7.2.1	Are access control systems in place on all system components?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Are access control systems configured to enforce privileges assigned to individuals based on job classification and function?	<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Do access control systems have a default "deny-all" setting? Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.	<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

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

PCI DSS Question		Response:		Special*
		Yes	No	
8.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? <ul style="list-style-type: none"> ▪ Something you know, such as a password or passphrase ▪ Something you have, such as a token device or smart card ▪ Something you are, such as a biometric 	<input type="checkbox"/>	<input type="checkbox"/>	
8.3	Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? <i>(For example, remote authentication and dial-in service (RADIUS) with tokens; or terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)</i> Note: Two-factor authentication requires that two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.	<input type="checkbox"/>	<input type="checkbox"/>	
8.4	(a) Are all passwords rendered unreadable during transmission and storage on all system components using strong cryptography?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For Service Providers only: Are customer passwords encrypted?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Are proper user identification and authentication management controls in place for non-consumer users and administrators on all system components, as follows:			
8.5.1	Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled, such that user IDs are implemented only as authorized (including with specified privileges)?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	Is user identity verified before performing password resets for user requests made via a non-face-to-face method (for example, phone, e-mail, or web)?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	Are first-time and reset passwords set to a unique value for each user, and must each user change their password immediately after the first use?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	Is access for any terminated users immediately deactivated or removed?	<input type="checkbox"/>	<input type="checkbox"/>	

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> *
8.5.5	Are inactive user accounts over 90 days old either removed or disabled?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	(a) Are accounts used by vendors for remote access, maintenance or support enabled only during the time period needed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are vendor remote access accounts monitored when in use?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Are authentication procedures and policies communicated to all users who have access to cardholder data?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	Are group, shared, or generic accounts and passwords, or other authentication methods, prohibited as follows: <ul style="list-style-type: none"> • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components 		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	(a) Are user passwords changed at least every 90 days?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For service providers only: Are non-consumer user passwords required to be changed periodically and are non-consumer users given guidance as to when, and under what circumstances, passwords must change?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	(a) Is a minimum password length of at least seven characters required?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For service providers only: Are non-consumer user passwords required to meet minimum length requirements?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	(a) Must passwords contain both numeric and alphabetic characters?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For service providers only: Are non-consumer user passwords required to contain both numeric and alphabetic characters?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	(a) Must an individual submit a new password that is different from any of the last four passwords he or she has used?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For service providers only: Are new, non-consumer user passwords required to be different from any of the last four passwords used?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	(a) Are repeated access attempts limited by locking out the user ID after no more than six attempts?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For service providers only: Are non-consumer user passwords temporarily locked-out after not more than six invalid access attempts?		<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:		Special*
		<u>Yes</u>	<u>No</u>	
8.5.14	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until administrator enables the user ID?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	(a) Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is all user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is user direct access or queries to databases restricted to database administrators?	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Are application IDs with database access only able to be used by the applications (and not by individual users or other processes)?	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response:		Special*
		Yes	No	
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) Are video cameras and/or access-control mechanisms in place to monitor individual physical access to sensitive areas? <i>Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are video cameras and/or access-control mechanisms protected from tampering or disabling?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries, and is data stored for at least three months, unless otherwise restricted by law?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	Is physical access to publicly accessible network jacks restricted (For example, areas accessible to visitors do not have network ports enabled unless network access is explicitly authorized)? Alternatively, are visitors escorted at all times in areas with active network jacks?	<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?	<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Are procedures developed to easily distinguish between onsite personnel and visitors, as follows: <i>For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>			
	(a) Do processes and procedures for assigning badges to onsite personnel and visitors include the following: <ul style="list-style-type: none"> • Granting new badges, • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor badges? 	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is access to the badge system limited to authorized personnel?	<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:		Special*
		Yes	No	
	(c) Do badges clearly identify visitors and easily distinguish between onsite personnel and visitors?	<input type="checkbox"/>	<input type="checkbox"/>	
9.3	Are all visitors handled as follows:			
9.3.1	Are visitors authorized before entering areas where cardholder data is processed or maintained?	<input type="checkbox"/>	<input type="checkbox"/>	
9.3.2	(a) Are visitors given a physical token (for example, a badge or access device) that identifies the visitors as not onsite personnel?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do visitor badges expire?	<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	Are visitors asked to surrender the physical token before leaving the facility or upon expiration	<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) Is a visitor log in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is the visitor log retained for at least three months?	<input type="checkbox"/>	<input type="checkbox"/>	
9.5	(a) Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is this location's security reviewed at least annually?	<input type="checkbox"/>	<input type="checkbox"/>	
9.6	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:			
9.7.1	Is media classified so the sensitivity of the data can be determined?	<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Is strict control maintained over the storage and accessibility of media?	<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	Are inventory logs of all media properly maintained and are periodic media inventories conducted at least annually?	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:		Special*
		Yes	No	
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?	<input type="checkbox"/>	<input type="checkbox"/>	
	Is destruction performed as follows:			
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a "to-be-shredded" container has a lock preventing access to its contents.)	<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Is cardholder data on electronic media rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media (for example, degaussing), so that cardholder data cannot be reconstructed?	<input type="checkbox"/>	<input type="checkbox"/>	

Regularly Monitor and Test Networks

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

PCI DSS Question		Response:		Special*
		Yes	No	
10.1	Is a process in place to link all access to system components (especially access done with administrative privileges such as root) to each individual user?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:			
10.2.1	All individual user accesses to cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	All actions taken by any individual with root or administrative privileges?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Access to all audit trails?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Invalid logical access attempts?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Use of identification and authentication mechanisms?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Initialization of the audit logs?	<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Creation and deletion of system-level object?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3	Are the following audit trail entries recorded for all system components for each event:			
10.3.1	User identification?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Type of event?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Date and time?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Success or failure indication?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origination of event?	<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identity or name of affected data, system component, or resource?	<input type="checkbox"/>	<input type="checkbox"/>	
10.4	(a) Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current? <i>Note: One example of time synchronization technology is Network Time Protocol (NTP).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are the following controls implemented for acquiring, distributing, and storing time:			
10.4.1	(a) Do only designated central time servers receive time signals from external sources, and do all critical systems have the correct and consistent time, based on International Atomic Time or UTC?	<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:		Special*
		Yes	No	
	(b) Do designated central time servers peer with each other to keep accurate time, and do other internal servers only receive time from the central time servers?	<input type="checkbox"/>	<input type="checkbox"/>	
10.4.2	Is time data is protected as follows:	<input type="checkbox"/>	<input type="checkbox"/>	
	(a) Access to time data is restricted to only personnel with a business need to access time data?			
	(b) Changes to time settings on critical systems are logged, monitored, and reviewed?	<input type="checkbox"/>	<input type="checkbox"/>	
10.4.3	Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	<input type="checkbox"/>	<input type="checkbox"/>	
10.5	Are audit trails secured so they cannot be altered, as follows:			
10.5.1	Is viewing of audit trails limited to those with a job-related need?	<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	<input type="checkbox"/>	<input type="checkbox"/>	
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) offloaded or copied onto a secure, centralized log server or media on the internal LAN?	<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	<input type="checkbox"/>	<input type="checkbox"/>	
10.6	Are logs for all system components reviewed at least daily, and are follow-ups to exceptions required? <i>Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).</i> Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	<input type="checkbox"/>	<input type="checkbox"/>	
10.7	(a) Are audit log retention policies and procedures in place and do they require that audit trail history is retained for at least one year?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are audit logs available for at least one year and are processes in place to immediately restore at least the last three months' logs for analysis?	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Response:		Special*
		Yes	No	
11.1	<p>(a) Is a documented process implemented to detect and identify wireless access points on a quarterly basis?</p> <p>Note: <i>Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.</i></p> <p><i>Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(b) Does the methodology detect and identify any unauthorized wireless access points, including at least the following:</p> <ul style="list-style-type: none"> • WLAN cards inserted into system components; • Portable wireless devices connected to system components (for example, by USB, etc.); • Wireless devices attached to a network port or network device? 	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(c) Is the process to identify unauthorized wireless access points performed at least quarterly for all system components and facilities?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(d) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to personnel?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>(e) Does the Incident Response Plan (Requirement 12.9) include a response in the event unauthorized wireless devices are detected?</p>	<input type="checkbox"/>	<input type="checkbox"/>	
11.2	<p>Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows?</p> <p>Note: <i>It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.</i></p>			

* “Not Applicable” (N/A) or “Compensating Control Used.” Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:		Special*
		Yes	No	
11.2.1	(a) Are quarterly internal vulnerability scans performed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Does the quarterly internal scan process include rescans until passing results are obtained, or until all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are internal quarterly scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	
11.2.2	(a) Are quarterly external vulnerability scans performed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do external quarterly scan results satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are quarterly external vulnerability scans performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC)?	<input type="checkbox"/>	<input type="checkbox"/>	
11.2.3	(a) Are internal and external scans performed after any significant change (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)? <i>Note: Scans conducted after network changes may be performed by internal staff.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Does the scan process include rescans until: <ul style="list-style-type: none"> For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS, For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved? 	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	
11.3	(a) Is external and internal penetration testing performed at least once a year and after any significant infrastructure or application changes (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are noted exploitable vulnerabilities corrected and testing repeated?	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:		Special*
		Yes	No	
	(c) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV).	<input type="checkbox"/>	<input type="checkbox"/>	
Do these penetration tests include the following:				
11.3.1	Network-layer penetration tests? <i>Note: The tests should include components that support network functions as well as operating systems.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Application-layer penetration tests? <i>Note: The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are IDS and/or IPS configured to alert personnel of suspected compromises?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Are file-integrity monitoring tools deployed within the cardholder data environment? Examples of files that should be monitored include: <ul style="list-style-type: none"> • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files 	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are the tools configured to alert personnel to unauthorized modification of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? <i>Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).</i>	<input type="checkbox"/>	<input type="checkbox"/>	

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Question	Response:	Response:		Special*
		Yes	No	
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel? <i>For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Does the policy address all PCI DSS requirements?	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	(a) Is an annual risk assessment process documented that identifies threats and vulnerabilities, and results in a formal risk assessment? (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the risk assessment process performed at least annually?	<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Is the information security policy reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment?	<input type="checkbox"/>	<input type="checkbox"/>	
12.2	Are daily operational security procedures developed that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures), and do they include administrative and technical procedures for each of the requirements?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3	Are usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all personnel, and require the following:			
12.3.1	Explicit approval by authorized parties to use the technologies?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentication for use of the technology?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	A list of all such devices and personnel with access?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Labeling of devices to determine owner, contact information, and purpose?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Acceptable uses of the technologies?	<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Acceptable network locations for the technologies?	<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question		Response:	Yes	No	Special*
12.3.7	List of company-approved products?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.10	(a) For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?		<input type="checkbox"/>	<input type="checkbox"/>	
	Are the following information security management responsibilities formally assigned to an individual or team:				
12.5.1	Establishing, documenting, and distributing security policies and procedures?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.4	Administering user accounts, including additions, deletions, and modifications?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5	Monitoring and controlling all access to data?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do security awareness program procedures include the following:				
12.6.1	(a) Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)?		<input type="checkbox"/>	<input type="checkbox"/>	
	Note: <i>Methods can vary depending on the role of the personnel and their level of access to the cardholder data.</i>				
	(b) Are personnel educated upon hire and at least annually?		<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:		Special*
		Yes	No	
12.6.2	Are personnel required to acknowledge at least annually that they have read and understood the security policy and procedures?	<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Are potential personnel (see definition of "personnel" at Requirement 12.1, above) screened prior to hire to minimize the risk of attacks from internal sources? (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) <i>Note: For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows:			
12.8.1	Is a list of service providers maintained?	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess?	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	<input type="checkbox"/>	<input type="checkbox"/>	
12.9	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:			
12.9.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Does the plan address, at a minimum:			
	▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Specific incident response procedures?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Business recovery and continuity procedures?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Data back-up processes?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Analysis of legal requirements for reporting compromises?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Coverage and responses of all critical system components?	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Reference or inclusion of incident response procedures from the payment brands?	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> *
12.9.2	Is the plan tested at least annually?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	Is appropriate training provided to staff with security breach response responsibilities?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	Are alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems included in the incident response plan?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?		<input type="checkbox"/>	<input type="checkbox"/>	

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect cardholder data environment

PCI DSS Question		Response:		Yes	No	Special*
A.1	<p>Is each entity's (that is, a merchant, service provider, or other entity) hosted environment and data protected, per A.1.1 through A.1.4 as follows:</p> <p><i>A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.</i></p> <p><i>Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.</i></p>					
A.1.1	<p>Does each entity run processes that have access to only that entity's cardholder data environment, and are these application processes run using the unique ID of the entity?</p> <p>For example:</p> <ul style="list-style-type: none"> No entity on the system can use a shared web server user ID. All CGI scripts used by an entity must be created and run as the entity's unique user ID 	<input type="checkbox"/>	<input type="checkbox"/>			
A.1.2	<p>Are each entity's access and privileges restricted to its own cardholder data environment as follows:</p>					
	(a) Are the user IDs for application processes not privileged users (root/admin)?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Does each entity have read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.)? <i>Important: An entity's files may not be shared by group.</i>	<input type="checkbox"/>	<input type="checkbox"/>			
	(c) Do all entities' users not have write access to shared system binaries?	<input type="checkbox"/>	<input type="checkbox"/>			
	(d) Is viewing of log entries restricted to the owning entity?	<input type="checkbox"/>	<input type="checkbox"/>			

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

PCI DSS Question	Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> [*]
(e) Are restrictions in place for the use of these system resources? <ul style="list-style-type: none"> • Disk space, • Bandwidth, • Memory, • CPU <i>This ensures that each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows),</i>		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3 Are logging and audit trails enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10? Is logging enabled as follows, for each merchant and service provider environment:		<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> • Logs are enabled for common third-party applications? 		<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> • Logs are active by default? 		<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> • Logs are available for review by the owning entity? 		<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> • Log locations are clearly communicated to the owning entity? 		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4 Are written policies and processes enabled to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider?		<input type="checkbox"/>	<input type="checkbox"/>	

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be “above and beyond” other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating “above and beyond” for compensating controls, consider the following:

Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

- a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
 - b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.
 - c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where “YES” was checked and compensating controls were mentioned in the “Special” column.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet—Completed Example

Use this worksheet to define compensating controls for any requirement where “YES” was checked and compensating controls were mentioned in the “Special” column.

Requirement Number: 8.1—*Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	<i>Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a “root” login. It is not possible for Company XYZ to manage the “root” login nor is it feasible to log all “root” activity by each user.</i>
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	<i>The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.</i>
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	<i>Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.</i>
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	<i>Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the “root” account and perform actions under the “root” account but is able to be logged in the SU-log directory. In this way, each user’s actions can be tracked through the SU account.</i>
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	<i>Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges</i>
6. Maintenance	Define process and controls in place to maintain compensating controls.	<i>Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged</i>

