



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

---

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

**Version 1.1**

February 2008

## Table of Contents

---

<b>PCI Data Security Standard: Related Documents .....</b>	<b>ii</b>
<b>Before You Begin .....</b>	<b>iii</b>
<b>Completing the Self-Assessment Questionnaire .....</b>	<b>iii</b>
<b>PCI DSS Compliance - Completion Steps .....</b>	<b>iii</b>
<b>Guidance for Exclusion of Certain, Specific Requirements .....</b>	<b>iv</b>
<b>Attestation of Compliance, SAQ D—Merchant Version .....</b>	<b>1</b>
<b>Attestation of Compliance, SAQ D—Service Provider Version.....</b>	<b>4</b>
<b>Self-Assessment Questionnaire D.....</b>	<b>7</b>
<b>Build and Maintain a Secure Network .....</b>	<b>7</b>
<i>Requirement 1: Install and maintain a firewall configuration to protect data .....</i>	<i>7</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .....</i>	<i>9</i>
<b>Protect Cardholder Data.....</b>	<b>11</b>
<i>Requirement 3: Protect stored cardholder data .....</i>	<i>11</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks ..</i>	<i>13</i>
<b>Maintain a Vulnerability Management Program.....</b>	<b>14</b>
<i>Requirement 5: Use and regularly update anti-virus software or programs.....</i>	<i>14</i>
<i>Requirement 6: Develop and maintain secure systems and applications.....</i>	<i>14</i>
<b>Implement Strong Access Control Measures .....</b>	<b>17</b>
<i>Requirement 7: Restrict access to cardholder data by business need-to-know.....</i>	<i>17</i>
<i>Requirement 8: Assign a unique ID to each person with computer access .....</i>	<i>17</i>
<i>Requirement 9: Restrict physical access to cardholder data.....</i>	<i>18</i>
<b>Regularly Monitor and Test Networks.....</b>	<b>21</b>
<i>Requirement 10: Track and monitor all access to network resources and cardholder data</i>	<i>21</i>
<i>Requirement 11: Regularly test security systems and processes .....</i>	<i>22</i>
<b>Maintain an Information Security Policy .....</b>	<b>24</b>
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors .....</i>	<i>24</i>
<b>PCI DSS Applicability for Hosting Providers .....</b>	<b>27</b>
<i>Requirement A.1: Hosting providers protect cardholder data environment .....</i>	<i>27</i>
<b>Compensating Controls Appendix .....</b>	<b>28</b>
<b>Compensating Controls for Requirement 3.4 .....</b>	<b>28</b>
<b>Compensating Controls Worksheet .....</b>	<b>29</b>
<b>Compensating Controls Worksheet—Completed Example .....</b>	<b>30</b>

---

## PCI Data Security Standard: Related Documents

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

Document	Audience
<i>PCI Data Security Standard</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>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Service providers and all other merchants <sup>1</sup>
<i>PCI DSS Glossary, Abbreviations, and Acronyms</i>	All merchants and service providers

<sup>1</sup> 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 SAQs A-C as described briefly in the table below and fully in *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*.

SAQ Validation Type	Description	SAQ
1	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>	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and <b>all</b> service providers defined by a payment brand as eligible to complete an SAQ.	D

These merchants not meeting the criteria for SAQs A-C above and all service providers defined by a payment brand as being SAQ-eligible are defined as SAQ Validation Type 5, here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*.

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 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 Data Security Standard.

### PCI DSS Compliance - Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ D) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete a clean vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.
3. Complete the Attestation of Compliance in its entirety.
4. 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 Exclusion of Certain, Specific Requirements

If you are required to answer SAQ D to validate your PCI DSS compliance, the following exceptions may be considered:

- The questions specific to wireless only need to be answered if wireless is present anywhere in your network (Requirements 1.3.8, 2.1.1, and 4.1.1). Note that Requirement 11.1 (use of wireless analyzer) must still be answered even if wireless is not in your network, since the analyzer detects any rogue or unauthorized devices that may have been added without the merchant's knowledge.
- The questions specific to custom applications and code (Requirements 6.3-6.5) only need to be answered if your organization writes its own custom web applications.
- The questions specific to data centers (Requirements 9.1-9.4), only need to be answered if you have a dedicated data center or server room. A data center is defined by PCI SSC as a dedicated, physically secure room or structure where information technology infrastructure (application servers, database servers, web servers, and/or network devices) is centrally housed, whose main purpose is to store, process, or transmit cardholder data. "Data center" may be synonymous with server room, network operations center (NOC), and co-location facilities at an ISP or hosting provider.

## 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). Complete all applicable sections and refer to the submission instructions at PCI DSS Compliance – Completion Steps in this document.

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

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

#### Part 2. Merchant Organization Information

Company Name:		DBA(S):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:					
State/Province:		Country:		ZIP:	
URL:					

#### Part 2a. 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 2b. Relationships

Does your company have a relationship with one or more third-party service providers (e.g. 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 2c. Transaction Processing

Payment Application in use:	Payment Application Version:
-----------------------------	------------------------------

#### 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 Scan Vendor, 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 Scan Vendor, 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:**

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | PCI DSS Self-Assessment Questionnaire D, Version ( <i>version of SAQ</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 in all material respects.   |
| <input type="checkbox"/> | I have confirmed with my POS vendor that my POS system does not store sensitive authentication data after authorization.   |
| <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 <sup>2</sup> , CAV2, CVC2, CID, or CVV2 data <sup>3</sup> , or PIN data <sup>4</sup> storage subsequent to 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> ↑

*Merchant Company Represented* ↑

<sup>2</sup> Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data subsequent to transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

<sup>3</sup> 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.

<sup>4</sup> 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	<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"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<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). Complete all applicable sections and refer to the submission instructions at PCI DSS Compliance – Completion Steps in this document.

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

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

### Part 2. Service Provider Organization Information

Company Name:			
Contact Name:	Title:		
Telephone:	E-mail:		
Business Address:			
State/Province:	Country:	ZIP:	
URL:			

### Part 2a. Services

#### Services Provided (check all that apply):

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Authorization   | <input type="checkbox"/> Loyalty Programs      | <input type="checkbox"/> 3-D Secure Access Control Server     |
| <input type="checkbox"/> Switching       | <input type="checkbox"/> IPSP (E-commerce)     | <input type="checkbox"/> Process Magnetic-Stripe Transactions |
| <input type="checkbox"/> Payment Gateway | <input type="checkbox"/> Clearing & Settlement | <input type="checkbox"/> Process MO/TO Transactions           |
| <input type="checkbox"/> Hosting         | <input type="checkbox"/> Issuing Processing    | <input type="checkbox"/> Others (please specify):             |

List facilities and locations included in PCI DSS review:

### Part 2b. Relationships

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

### Part 2c: Transaction Processing

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

Payment Applications in use or provided as part of your service:	Payment Application Version:
--	------------------------------

### 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 Scan Vendor, 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 Scan Vendor, 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:

- Self-Assessment Questionnaire D, Version (*insert version number*), 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.
- 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) data<sup>5</sup>, CAV2, CVC2, CID, or CVV2 data<sup>6</sup>, or PIN data<sup>7</sup> storage subsequent to 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> ↑

*Service Provider Company Represented* ↑

<sup>5</sup> Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data subsequent to transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

<sup>6</sup> 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.

<sup>7</sup> 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	<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"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	

## Self-Assessment Questionnaire D

Date of Completion:

### Build and Maintain a Secure Network

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

Question		Response:	Yes	No	Special*
1.1	Do established firewall configuration standards include the following?				
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall configuration?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	A current network diagram with all connections to cardholder data, including any wireless networks?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.3	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"/>	
1.1.4	Description of groups, roles, and responsibilities for logical management of network components?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.5	Documented list of services and ports necessary for business?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.7	Justification and documentation for any risky protocols allowed (for example, file transfer protocol [FTP]), which includes reason for use of protocol and security features implemented?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.8	Quarterly review of firewall and router rule sets?		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.9	Configuration standards for routers?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2	Does the firewall configuration deny all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder environment?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3	(a) Does the firewall configuration restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks?  (b) Does the firewall configuration:		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	Yes	No	Special*
1.3.1	Restrict inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	Prohibit the passing of internal addresses from the Internet into the DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	Implement stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	Place the database in an internal network zone, segregated from the DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	Secure and synchronize router configuration files? (For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration.)		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	Deny all other inbound and outbound traffic not specifically allowed?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	Include installation of perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
1.3.9	Include installation of personal firewall software on any mobile and 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"/>	
1.4	(a) Does the firewall configuration prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files), (b) At a minimum, do controls ensure the following?		<input type="checkbox"/>	<input type="checkbox"/>	
1.4.1	Has a DMZ been implemented to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic?		<input type="checkbox"/>	<input type="checkbox"/>	
1.4.2	Is outbound traffic restricted from payment card applications to IP addresses within the DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.5	Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet? <i>Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).</i>		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		Response: <u>Yes</u> <u>No</u>		<u>Special*</u>
2.1	Are vendor-supplied defaults always changed <b>before</b> installing a system on the network? <i>Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	Are wireless environment defaults changed before installing a wireless system? <i>Wireless environment defaults include but are not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(a) Are SSID broadcasts disabled?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is WiFi protected access (WPA and WPA2) technology enabled for encryption and authentication when WPA-capable?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Have configuration standards been developed for all system components?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do these standards address all known security vulnerabilities and are they consistent with industry-accepted system hardening standards—as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Do controls ensure the following?			
2.2.1	Is only one primary function implemented per server (for example, web servers, database servers, and DNS should be implemented on separate servers)?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Are all unnecessary and insecure services and protocols disabled (services and protocols not directly needed to perform the devices' specified function)?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Are system security parameters configured to prevent misuse?	<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	<input type="checkbox"/>	<input type="checkbox"/>	

\* “Not Applicable” (permitted only when indicated) or “Compensating Control Used.” Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
2.3	Is all non-console administrative access encrypted? <i>Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.4	If you are a hosting provider, are your systems configured to protect each entity's hosted environment and data? <i>See Appendix A: "PCI DSS Applicability for Hosting Providers" for specific requirements that must be met.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

---

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

## Protect Cardholder Data

### Requirement 3: *Protect stored cardholder data*

Question		Response:	Yes	No	Special*
3.1	(a) Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and/or regulatory purposes?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.		<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>Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).</i>		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	Yes	No	Special*
3.4	<p>Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches?</p> <ul style="list-style-type: none"> <li>– Strong one-way hash functions (hashed indexes)</li> <li>– Truncation</li> <li>– Index tokens and pads (pads must be securely stored)</li> <li>– Strong cryptography with associated key management processes and procedures.</li> </ul> <p><b>The MINIMUM account information that must be rendered unreadable is the PAN.</b></p> <p><i>If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls for Encryption of Stored Data."</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	<p>If disk encryption (rather than file- or column-level database encryption) is used:</p> <p>(a) Is logical access managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts)?</p> <p>(b) Are decryption keys independent of user accounts?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	Are encryption keys used for encryption of cardholder data protected against both disclosure and misuse?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	Is access to keys restricted to the fewest number of custodians necessary?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	Are keys stored securely, and in the fewest possible locations and forms?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6	<p>(a) Are all key-management processes and procedures for keys used for encryption of cardholder data, fully documented and implemented?</p> <p>(b) Do they include the following?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.1	Generation of strong keys		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Secure key distribution		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Secure key storage		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	<p>Periodic changing of keys</p> <ul style="list-style-type: none"> <li>– As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically</li> <li>– At least annually.</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Destruction of old keys		<input type="checkbox"/>	<input type="checkbox"/>	

Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Prevention of unauthorized substitution of keys	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Replacement of known or suspected compromised keys	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.9	Revocation of old or invalid keys	<input type="checkbox"/>	<input type="checkbox"/>	
3.6.10	Requirement for key custodians to sign a form stating 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**

4.1	Are strong cryptography and security protocols, such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC), used to safeguard sensitive cardholder data during transmission over open, public networks?  <i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i>	<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	(a) For wireless networks transmitting cardholder data, are transmissions encrypted by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS?  <i>Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) If WEP is used, do controls ensure the following?			
	- WEP is used with a minimum 104-bit encryption key and 24 bit-initialization value.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	- WEP is used ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	- Shared WEP keys are rotated quarterly (or automatically if the technology permits).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	- Shared WEP keys are rotated whenever there are changes in personnel with access to keys.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	- Access is restricted based on media access code (MAC) address.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by e-mail?	<input type="checkbox"/>	<input type="checkbox"/>	

## Maintain a Vulnerability Management Program

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

Question		Response:		Special*
		Yes	No	
5.1	Is anti-virus software deployed on all systems commonly affected by viruses (particularly personal computers and servers)? <i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware?	<input type="checkbox"/>	<input type="checkbox"/>	
5.2	Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?	<input type="checkbox"/>	<input type="checkbox"/>	

### Requirement 6: Develop and maintain secure systems and applications

6.1	(a) Do all system components and software have the latest vendor-supplied security patches installed?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are relevant security patches installed within one month of release?	<input type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) Is there a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet)?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are standards appropriately updated to address new vulnerability issues?	<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Are software applications developed based on industry best practices, and do they incorporate information security throughout the software development life cycle.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) Do controls ensure the following?			
6.3.1	Testing of all security patches and system and software configuration changes before deployment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.2	Separate development, test, and production environments?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.3	Separation of duties between development, test, and production environments?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.4	Production data (live PANs) are not used for testing or development?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.5	Removal of test data and accounts before production systems become active?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

\* “Not Applicable” (permitted only when indicated) or “Compensating Control Used.” Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:		Special*
		Yes	No	
6.3.6	Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4	(a) Are change control procedures followed for all system and software configuration change?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) Do controls ensure the following?			
6.4.1	Documentation of impact?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.2	Management sign-off by appropriate parties?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.3	Testing of operational functionality?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.4.4	Back-out procedures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5	(a) Are all web applications developed based on secure coding guidelines such as the Open Web Application Security Project guidelines?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) Is custom application code reviewed to identify coding vulnerabilities?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(c) Is prevention of common coding vulnerabilities covered in software development processes, including the following?			
6.5.1	Unvalidated input?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.2	Broken access control (for example, malicious use of user IDs)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.3	Broken authentication and session management (use of account credentials and session cookies)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.4	Cross-site scripting (XSS) attacks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.5	Buffer overflows?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.6	Injection flaws (for example, structured query language (SQL) injection)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.7	Improper error handling?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

\* “Not Applicable” (permitted only when indicated) or “Compensating Control Used.” Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
6.5.8	Insecure storage?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.9	Denial of service?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.5.10	Insecure configuration management?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
6.6	<p>Are all web-facing applications protected against known attacks by applying either of the following methods?</p> <ul style="list-style-type: none"> <li>– Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security.</li> <li>– Installing an application layer firewall in front of web-facing applications.</li> </ul> <p><i>Note: 6.6 is considered a best practice until June 30, 2008, after which it becomes a requirement.</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

	Question	Response:	Yes	No	Special*
7.1	Is access to computing resources and cardholder information limited to only those individuals whose jobs require such access?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	For systems with multiple users, is a mechanism in place to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed?		<input type="checkbox"/>	<input type="checkbox"/>	

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

8.1	Are all users identified with a unique user name 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"> <li>– Password</li> <li>– Token devices (e.g., SecureID, certificates, or public key)</li> <li>– Biometrics</li> </ul>		<input type="checkbox"/>	<input type="checkbox"/>	
8.3	Is two-factor authentication implemented for remote access to the network by employees, administrators, and third parties? <i>Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
8.4	Are all passwords encrypted during transmission and storage on all system components?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5	Are proper user authentication and password management controls in place for non-consumer users and administrators on all system components, as follows?				
8.5.1	Are addition, deletion, and modification of user IDs, credentials, and other identifier objects controlled?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	Is user identity verified before performing password resets?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	Are first-time 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 revoked?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	Are inactive user accounts removed at least every 90 days?		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:		Special*
		Yes	No	
8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Are password 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 not permitted?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	Must user passwords be changed at least every 90 days?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	Is a minimum password length of at least seven characters required?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.11	Must passwords contain both numeric and alphabetic characters?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	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"/>	
8.5.13	Are repeated access attempts limited by locking out the user ID after no more than six attempts?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.14	Is the lockout duration set to thirty 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, must the user re-enter the password to re-activate the terminal?	<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	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"/>	

**Requirement 9: Restrict physical access to cardholder data**

9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems that store, process, or transmit cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.1	(a) Do cameras monitor sensitive areas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) Is data from video cameras audited and correlated with other entries?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(c) Is data from video cameras stored for at least three months, unless otherwise restricted by law?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.2	Is physical access to publicly accessible network jacks restricted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.1.3	Is physical access to wireless access points, gateways, and handheld devices restricted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:		Special*
		Yes	No	
9.2	<p>Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible?</p> <p><i>“Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3	Are all visitors handled as follows:			
9.3.1	Authorized before entering areas where cardholder data is processed or maintained?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.4	(a) Is a visitor log in use to maintain a physical audit trail of visitor activity?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
	(b) Is visitor log retained for a minimum of three months, unless otherwise restricted by law?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> N/A
9.5	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"/>	
9.6	<p>Are all paper and electronic media that contain cardholder data physically secure?</p> <p><i>(Such media includes computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes.)</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:			
9.7.1	Is the media classified so it can be identified as confidential?	<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately tracked?	<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media from a secured area (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 that contains cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>	
9.9.1	Is all media properly inventoried and securely stored?	<input type="checkbox"/>	<input type="checkbox"/>	

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Are hardcopy materials cross-cut shredded, incinerated, or pulped?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Is electronic media purged, degaussed, shredded, or otherwise destroyed 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*

Question		Response:	Yes	No	Special*
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:		<input type="checkbox"/>	<input type="checkbox"/>	
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	Are all critical system clocks and times synchronized?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) Are audit trails secured so they cannot be altered?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls ensure the following?				
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?		<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"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	Yes	No	Special*
10.5.4	Are logs for wireless networks copied onto a log server on the internal LAN?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Are file integrity monitoring and 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? <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> <b>Note:</b> Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	Is audit trail history retained for at least one year, with a minimum of three months online availability?		<input type="checkbox"/>	<input type="checkbox"/>	

**Requirement 11: Regularly test security systems and processes**

11.1	(a) Are security controls, limitations, network connections, and restrictions tested annually to assure the ability to adequately identify and to stop any unauthorized access attempts?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is a wireless analyzer used at least quarterly to identify all wireless devices in use?		<input type="checkbox"/>	<input type="checkbox"/>	
11.2	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)? <b>Note:</b> Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.		<input type="checkbox"/>	<input type="checkbox"/>	
11.3	(a) Is penetration testing performed at least once a year and after any significant infrastructure or application upgrade or modification (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) Do these penetration tests include the following:				
11.3.1	Network-layer penetration tests?		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Application-layer penetration tests?		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:		Special*
		Yes	No	
11.4	(a) Are network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems used to monitor all network traffic and alert personnel to suspected compromises?	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are all intrusion detection and prevention engines kept up-to-date?	<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Is file integrity monitoring software deployed to alert personnel to unauthorized modification of critical system or content files; and	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the software configured to perform critical file comparisons at least weekly? <i>Critical files are not necessarily only those containing cardholder data. 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 employees and contractors*

Question		Response:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Addresses all requirements in this specification?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2	Includes an annual process to identify threats and vulnerabilities, and which results in a formal risk assessment?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Includes a review at least once a year and updates when the environment changes?		<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)?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Are usage policies for critical employee-facing technologies (such as modems and wireless) developed to define proper use of these technologies for all employees and contractors?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do these usage policies require the following?				
12.3.1	Explicit management approval?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentication for use of the technology?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	List of all such devices and personnel with access?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Labeling of devices with 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"/>	
12.3.7	List of company-approved products?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Automatic disconnect of modem sessions after a specific period of inactivity?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Activation of modems for vendors only when needed by vendors, with immediate deactivation after use?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.10	When accessing cardholder data remotely via modem, does the policy specify the following?				
	(a) Prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media?		<input type="checkbox"/>	<input type="checkbox"/>	

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

Question		Response:	Yes	No	Special*
	(b) Prohibition of cut-and-paste and print functions during remote access?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Are the following information security management responsibilities 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	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.1	Are employees educated upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Are employees required to acknowledge in writing that they have read and understood the company's security policy and procedures?		<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Are potential employees screened to minimize the risk of attacks from internal sources? <i>For those employees 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	Contractually, are the following required if cardholder data is shared with service providers?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	That service providers must adhere to the PCI DSS requirements?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	An agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses?		<input type="checkbox"/>	<input type="checkbox"/>	

Question		Response:		Yes	No	Special*
12.9	Has an incident response plan been implemented to include the following?					
12.9.1	(a) Has an incident response plan been created to be implemented in the event of system compromise?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Does the plan address, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the acquirers and payment card associations)?	<input type="checkbox"/>	<input type="checkbox"/>			
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?	<input type="checkbox"/>	<input type="checkbox"/>			
12.9.6	Is 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"/>			
12.10	(a) Do all processors and service providers maintain and implement policies and procedures to manage connected entities?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Do controls include the following:					
12.10.1	A list of connected entities?	<input type="checkbox"/>	<input type="checkbox"/>			
12.10.2	Assurance that proper due diligence is conducted prior to connecting an entity?	<input type="checkbox"/>	<input type="checkbox"/>			
12.10.3	Assurance that the entity is PCI DSS compliant?	<input type="checkbox"/>	<input type="checkbox"/>			
12.10.4	Entities are connected and disconnected by following an established process?	<input type="checkbox"/>	<input type="checkbox"/>			

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

## PCI DSS Applicability for Hosting Providers

### *Requirement A.1: Hosting providers protect cardholder data environment*

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
A.1	Is each entity's (that is, a merchant, service provider, or other entity) hosted environment and data protected, as in A.1.1 through A.1.4:				
A.1.1	Does each entity have access to only its own cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>		
A.1.2	Are each entity's access and privileges restricted to its own cardholder data environment?	<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?	<input type="checkbox"/>	<input type="checkbox"/>		
A.1.4	Are 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"/>		

\* "Not Applicable" (permitted only when indicated) or "Compensating Control Used." Organizations using compensating controls must complete the Compensating Control Worksheet in the Appendix.

## Compensating Controls Appendix

---

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the *PCI DSS Glossary* for the full definition of compensating controls.

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. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness.

The following guidance provides compensating controls when companies are unable to render cardholder data unreadable per requirement 3.4.

### Compensating Controls for Requirement 3.4

For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. *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.*

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the “Compensating Controls” definition in the *PCI DSS Glossary*. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all** of the following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer).
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
  - IP address/Mac address
  - Application/service
  - User accounts/groups
  - Data type (packet filtering)
3. Restrict logical access to the database.
  - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

## Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where “NO” 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. <b>Constraints</b>	List constraints precluding compliance with the original requirement.	
2. <b>Objective</b>	Define the objective of the original control; identify the objective met by the compensating control.	
3. <b>Identified Risk</b>	Identify any additional risk posed by the lack of the original control.	
4. <b>Definition of Compensating Controls</b>	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	

## Compensating Controls Worksheet—Completed Example

Use this worksheet to define compensating controls for any requirement where “NO” 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
<b>1. Constraints</b>	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>
<b>2. Objective</b>	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>
<b>3. Identified Risk</b>	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>
<b>4. Definition of Compensating Controls</b>	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>