



**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 1.2

October 2008

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.

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 and Exclusion of Certain, Specific Requirements	v
Attestation of Compliance, SAQ D—Merchant Version	1
Attestation of Compliance, SAQ D—Service Provider Version	4
Self-Assessment Questionnaire D	7
Build and Maintain a Secure Network	7
<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>
Protect Cardholder Data	11
<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>
Maintain a Vulnerability Management Program	14
<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>
Implement Strong Access Control Measures	17
<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>19</i>
Regularly Monitor and Test Networks	21
<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>
Maintain an Information Security Policy	24
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors</i>	<i>24</i>
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers 27	
<i>Requirement A.1: Shared hosting providers must protect cardholder data environment</i>	<i>27</i>
Appendix B: Compensating Controls	28
Appendix C: Compensating Controls Worksheet	29
Compensating Controls Worksheet—Completed Example	30
Appendix D: Explanation of Non-Applicability	31

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 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>	Merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Merchants ¹ and all service providers
<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 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 all 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 passing 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 Non-Applicability and Exclusion 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 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 for Requirements 9.1-9.4 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.

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 the Appendix 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. 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. Merchant Organization Information

Company Name:	DBA(S):		
Contact Name:	Title:		
Telephone:	E-mail:		
Business Address:	City:		
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 (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 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:

- 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> ↑

Merchant Company Represented ↑

² Data encoded in the magnetic stripe 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	<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	<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. 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. Service Provider Organization Information

Company Name:							
Contact Name:				Title:			
Telephone:				E-mail:			
Business Address:				City:			
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 (for example, 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:

- | | |
|--------------------------|--|
| <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> ↑

Service Provider Company Represented ↑

⁵ Data encoded in the magnetic stripe 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.

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"/>	
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	<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 and router configuration standards include the following?				
1.1.1	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	Current network diagrams 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	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure?	<input type="checkbox"/>	<input type="checkbox"/>		
1.1.6	Requirement to review firewall and router rule sets at least every six months)?	<input type="checkbox"/>	<input type="checkbox"/>		
1.2	Does the firewall configuration 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	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?	<input type="checkbox"/>	<input type="checkbox"/>		
1.2.2	Secure and synchronize router configuration files?	<input type="checkbox"/>	<input type="checkbox"/>		
1.2.3	Include installation of perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls 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"/>		

* "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.

Question		Response:	Yes	No	Special*
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?				
1.3.1	Is a DMZ implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder environment?	<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 routes 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 restricted from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ?	<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	Is the database placed in an internal network zone, segregated from the DMZ?	<input type="checkbox"/>	<input type="checkbox"/>		
1.3.8	Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space? <i>Use Network address translation (NAT) technologies—for example, port address translation (PAT).</i>	<input type="checkbox"/>	<input type="checkbox"/>		
1.4	Has personal firewall software been installed 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"/>		

* "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 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 before 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	(a) Are defaults** for wireless environments connected to the cardholder data environment or transmitting cardholder data changed before installing a wireless system? <i>** Such wireless environment defaults include but are not limited to default wireless encryption keys, passwords, and SNMP community strings.</i>	<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are wireless device security settings enabled for strong encryption technology for authentication and transmissions?	<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—for example, SysAdmin Audit Network Security (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?	<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 device's 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"/>	
2.3	Is all non-console administrative access encrypted? <i>Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</i>	<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.

	Question	Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
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

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 after authorization (even if encrypted)?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><i>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i></p> <ul style="list-style-type: none"> ▪ The cardholder's name, ▪ Primary account number (PAN), ▪ Expiration date, and ▪ Service code <p><i>To minimize risk, store only these data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>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.</p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>		<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	<p>Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)?</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ <i>This requirement does not apply to employees and other parties with a specific need to see the full PAN;</i> ▪ <i>This requirement does not 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" (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.

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, and in logs,) by using any of the following approaches?</p> <ul style="list-style-type: none"> ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. <p><i>The MINIMUM account information that must be rendered unreadable is the PAN.</i></p> <p><i>If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: "Compensating Controls."</i></p> <p><i>Note: "Strong cryptography" is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used:				
	(a) Is logical access 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 decryption keys independent of user accounts?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	Are cryptographic 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 cryptographic keys restricted to the fewest number of custodians necessary?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	Are cryptographic keys stored securely, and in the fewest possible locations and forms?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6	(a) Are all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, fully documented and implemented?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do they include the following?				
3.6.1	Generation of strong cryptographic keys		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Secure cryptographic key distribution		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Secure cryptographic key storage		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Periodic changing of cryptographic keys: <ul style="list-style-type: none"> ▪ As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically ▪ At least annually 		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Split knowledge and establishment of dual control of cryptographic keys		<input type="checkbox"/>	<input type="checkbox"/>	

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
3.6.7	Prevention of unauthorized substitution of cryptographic keys		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Requirement for cryptographic-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

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
4.1	Are strong cryptography and security protocols, such as SSL/TLS or 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, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
4.1.1	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? <i>Notes:</i> <ul style="list-style-type: none"> ▪ <i>For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</i> ▪ <i>For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</i> 		<input type="checkbox"/>	<input type="checkbox"/>	
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?		<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

Question		Response:		Yes	No	Special*
5.1	Is anti-virus software deployed on all systems, particularly personal computers and servers, 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?	<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

Question		Response:		Yes	No	Special*
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 critical security patches installed within one month of release? <i>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.</i>	<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 configuration standards updated as required by PCI DSS Requirement 2.2 to address new vulnerability issues?	<input type="checkbox"/>	<input type="checkbox"/>			
6.3	(a) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and do they incorporate information security throughout the software development life cycle?	<input type="checkbox"/>	<input type="checkbox"/>			
	(b) Do controls ensure the following?					
6.3.1	Testing of all security patches and system and software configuration changes before deployment, including but not limited to the following:	<input type="checkbox"/>	<input type="checkbox"/>			
6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	<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.

Question		Response:	Yes	No	Special*
6.3.1.2	Validation of proper error handling		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validation of secure cryptographic storage		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validation of secure communications		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validation of proper role-based access control (RBAC)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Separate development/test and production environments?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Separation of duties between development/test and production environments?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Production data (live PANs) are not used for testing or development?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Removal of test data and accounts before production systems become active?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability? <i>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel. 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.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) Are change control procedures followed for all changes to system components?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do procedures ensure the following?				
6.4.1	Documentation of impact?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Management sign-off by appropriate parties?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Testing of operational functionality?		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Back-out procedures?		<input type="checkbox"/>	<input type="checkbox"/>	

Question		Response:	Yes	No	Special*
6.5	(a) Are all web applications (internal and external, and including web administrative access to application) developed based on secure coding guidelines such as the <i>Open Web Application Security Project Guide</i> ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is prevention of common coding vulnerabilities covered in software development processes, including the following? <i>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</i>				
6.5.1	Cross-side scripting (XSS)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Injection flaws, particularly SQL injection? <i>Also consider LDAP and Xpath injection flaws as well as other injection flaws.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Malicious file execution?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Insecure direct object references?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Cross-site request forgery (CSRF)?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Information leakage and improper error handling?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Broken authentication and session management?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Insecure cryptographic storage?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Insecure communications?		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Failure to restrict URL access?		<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, at least annually and after any changes; or ▪ Installing a web-application layer firewall in front of public-facing web applications. 		<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.

Implement Strong Access Control Measures

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

Question		Response:	Yes	No	Special*
7.1	(a) Is access to system components and cardholder data limited to only those individuals whose jobs require such access?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do access limitations include the following:				
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Assignment of privileges based on individual personnel's job classification and function?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Requirement for an authorization form signed by management that specifies required privileges?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementation of an automated access control system?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) 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?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Does this access control system include the following:				
7.2.1	Coverage of all system components?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Assignment of privileges to individuals based on job classification and function?		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Default "deny-all" setting?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Question		Response:	Yes	No	Special*
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"> ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 		<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.

Question		Response:	Yes	No	Special*
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>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 rendered unreadable during transmission and storage on all system components using strong cryptography (defined in <i>PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms</i>)?		<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 or disabled at least every 90 days?		<input type="checkbox"/>	<input type="checkbox"/>	
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 prohibited?		<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"/>	

* “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.

Question		Response:	Yes	No	Special*
8.5.14	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, 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

Question		Response:	Yes	No	Special*
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) Do video cameras or other access-control mechanisms 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) Is data collected from video cameras reviewed and correlated with other entries?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is data from video cameras 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?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.3	Is physical access to wireless access points, gateways, and handheld devices restricted?		<input type="checkbox"/>	<input type="checkbox"/>	
9.2	Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible? <i>For purposes of this requirement, an "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors 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>		<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	

* "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.

Question		Response:	Yes	No	Special*
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"/>	
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"/>	
9.4	(a) Is a visitor log in use to maintain a physical audit trail of visitor activity?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are the visitor's name, the firm represented, and the employee authorizing physical access documented on the log?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is visitor log retained for a minimum of three months, unless otherwise restricted by law?		<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 paper and electronic media that contain cardholder data physically secure?		<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 containing cardholder data 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	(a) Are inventory logs of all media properly maintained?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are media inventories conducted at least annually?		<input type="checkbox"/>	<input type="checkbox"/>	
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 shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Is electronic media with cardholder data rendered unrecoverable 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:				
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" (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.

Question		Response:	Yes	No	Special*
10.5.4	Are logs for external-facing technologies written onto a log server 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? <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> <i>Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	Is audit trail history retained for at least one year, with a minimum of three months' history immediately available for analysis (for examples, online, archived, or restorable from backup)?		<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 11: Regularly test security systems and processes

Question		Response:	Yes	No	Special*
11.1	Is the presence of wireless access points tested for by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS 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)? <i>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.</i>		<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 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" (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.

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
11.4	(a) Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic in the cardholder data environment 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 files, configuration files, or content files; and		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the software configured to 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 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 PCI DSS requirements?		<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 (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) 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	A 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 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 only when needed by vendors, with immediate deactivation after use?		<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.

Question		Response:	Yes	No	Special*
12.3.10	When 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?		<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?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Are employees required to acknowledge at least annually that they have read and understood the company's security policy and procedures?		<input type="checkbox"/>	<input type="checkbox"/>	
12.7	Are potential employees (see definition of "employee" at 9.2 above) screened prior to hire 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	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	A list of service providers is maintained.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	A written agreement is 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"/>	

* "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.

Question		Response:	Yes	No	Special*
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.		<input type="checkbox"/>	<input type="checkbox"/>	
12.9	Has an incident response plan been implemented to include the following in preparation to respond immediately to a system breach?				
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"/>	
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"/>	

* "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.

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

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

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:</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	Does each entity run processes that have access to only that entity's 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" (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.

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>
7. 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>
8. 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>

