



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

**Payment Application Connected to Internet,
No Electronic Cardholder Data Storage**

Version 2.0

October 2010

Document Changes

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

Table of Contents

Document Changes	i
PCI Data Security Standard: Related Documents	iii
Before you Begin	iv
Completing the Self-Assessment Questionnaire	iv
PCI DSS Compliance – Completion Steps	v
Guidance for Non-Applicability of Certain, Specific Requirements	v
Attestation of Compliance, SAQ C	1
Self-Assessment Questionnaire C	5
Build and Maintain a Secure Network	5
<i>Requirement 1: Install and maintain a firewall configuration to protect data</i>	<i>5</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</i>	<i>6</i>
Protect Cardholder Data	7
<i>Requirement 3: Protect stored cardholder data</i>	<i>7</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks</i>	<i>8</i>
Maintain a Vulnerability Management Program	9
<i>Requirement 5: Use and regularly update anti-virus software or programs</i>	<i>9</i>
<i>Requirement 6: Develop and maintain secure systems and applications</i>	<i>9</i>
Implement Strong Access Control Measures	10
<i>Requirement 7: Restrict access to cardholder data by business need to know</i>	<i>10</i>
<i>Requirement 8: Assign a unique ID to each person with computer access</i>	<i>10</i>
<i>Requirement 9: Restrict physical access to cardholder data</i>	<i>10</i>
Regularly Monitor and Test Networks	12
<i>Requirement 11: Regularly test security systems and processes</i>	<i>12</i>
Maintain an Information Security Policy	14
<i>Requirement 12: Maintain a policy that addresses information security for all personnel</i>	<i>14</i>
Appendix A: (not used)	16
Appendix B: Compensating Controls	17
Appendix C: Compensating Controls Worksheet	18
Compensating Controls Worksheet—Completed Example	19
Appendix D: Explanation of Non-Applicability	20

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>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Eligible merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Eligible merchants and service providers ¹
<i>PCI Data Security Standard and Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms</i>	All merchants and service providers

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

Before you Begin

Completing the Self-Assessment Questionnaire

SAQ C has been developed to address requirements applicable to merchants who process cardholder data via payment applications (for example, point-of-sale systems) connected to the Internet (for example, via DSL, cable modem, etc.), but who do not store cardholder data on any computer system. These payment applications are connected to the Internet either because:

1. The payment application is on a personal computer connected to the Internet, or
2. The payment application is connected to the Internet to transmit cardholder data.

SAQ C merchants are defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. SAQ C merchants process cardholder data via POS machines or other payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. Such merchants validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- The payment application/Internet device is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- Your company store is not connected to other store locations, and any LAN is for a single store only;
- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; and
- Your company's payment application vendor uses secure techniques to provide remote support to your payment system.

Each section of this questionnaire focuses on a specific area of security, based on the requirements in the *PCI DSS Requirements and Security Assessment Procedures*. This shortened version of the SAQ includes questions which apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment which are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

PCI DSS Compliance – Completion Steps

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

Guidance for Non-Applicability of Certain, Specific Requirements

Exclusion: If you are required to answer SAQ C to validate your PCI DSS compliance, the following exception 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 a process to identify unauthorized wireless access points) must still be answered even if wireless is not in your network, since the process detects any rogue or unauthorized devices that may have been added without the your knowledge.

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

Attestation of Compliance, SAQ C

Instructions for Submission

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

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

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

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

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

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

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

List facilities and locations included in PCI DSS review:

Part 2a. Relationships

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

Part 2b. Transaction Processing

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

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

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

Part 2c. Eligibility to Complete SAQ C

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- Merchant has a payment application system and an Internet or public network connection on the same device and/or same local area network (LAN);
- The payment application system/Internet device is not connected to any other system within the merchant environment;
- Merchant store is not connected to other store locations, and any LAN is for a single store only;
- Merchant does not store cardholder data in electronic format;
- If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; **and**
- Merchant's payment application software vendor uses secure techniques to provide remote support to merchant's payment application system.

Part 3. PCI DSS Validation

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

- Compliant:** All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall **COMPLIANT** rating, **and** a passing scan has been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Merchant Company Name*) has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*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 C, 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 payment application vendor that my payment 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 ² , CAV2, CVC2, CID, or CVV2 data ³ , or PIN data ⁴ 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 or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

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

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

Part 4. Action Plan for Non-Compliant Status

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

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

Self-Assessment Questionnaire C

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

Date of Completion:

Build and Maintain a Secure Network

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

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
1.2 Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows: <i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>				
1.2.1 (a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment, and are the restrictions documented?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3 Are perimeter firewalls installed between any wireless networks and the cardholder data environment, and are these firewalls configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3 Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment, as follows:				
1.3.3 Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5 Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6 Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?		<input type="checkbox"/>	<input type="checkbox"/>	

* "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

PCI DSS Question		Response:	Yes	No	Special*
2.1	Are vendor-supplied defaults always changed before installing a system on the network? <i>Vendor-supplied defaults Include but are not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are defaults changed as follows:				
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are default SNMP community strings on wireless devices changed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Are default passwords/passphrases on access points changed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?		<input type="checkbox"/>	<input type="checkbox"/>	
	(e) Are other security-related wireless vendor defaults changed, if applicable?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?		<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Is all non-console administrative access encrypted as follows: <i>Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</i>				
	(a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?		<input type="checkbox"/>	<input type="checkbox"/>	

* "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.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
3.2 (b) If sensitive authentication data is received and deleted, are processes in place to securely delete the data to verify that the data is unrecoverable?		<input type="checkbox"/>	<input type="checkbox"/>	
(c) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted)?				
3.2.1 The full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance? This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i> <ul style="list-style-type: none"> ▪ <i>The cardholder's name,</i> ▪ <i>Primary account number (PAN),</i> ▪ <i>Expiration date, and</i> ▪ <i>Service code</i> <i>To minimize risk, store only these data elements as needed for business.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2 The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3 The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance?		<input type="checkbox"/>	<input type="checkbox"/>	
3.3 Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)? <i>Notes:</i> <ul style="list-style-type: none"> ▪ <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.

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

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

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

Maintain a Vulnerability Management Program

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

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

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
6.1	(a) Are all system components and software protected from known vulnerabilities by having the latest vendor-supplied security patches installed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are critical security patches installed within one month of release?		<input type="checkbox"/>	<input type="checkbox"/>	

* “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

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
7.1 (a) Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:				
7.1.1 Are access rights for privileged user IDs restricted to least privileges necessary to perform job responsibilities?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2 Are privileges assigned to individuals based on job classification and function (also called "role-based access control" or RBAC)?		<input type="checkbox"/>	<input type="checkbox"/>	

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

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
8.3 Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? <i>(For example, remote authentication and dial-in service (RADIUS) with tokens; or terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)</i> Note: Two-factor authentication requires that two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6 (a) Are accounts used by vendors for remote access, maintenance or support enabled only during the time period needed?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Are vendor remote access accounts monitored when in use?		<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
9.6 Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

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

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> *
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:				
9.7.1	Is media classified so the sensitivity of the data can be determined?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (especially when media is distributed to individuals)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9	Is strict control maintained over the storage and accessibility of media?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?		<input type="checkbox"/>	<input type="checkbox"/>	
	Is destruction performed as follows:				
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a "to-be-shredded" container has a lock preventing access to its contents.)		<input type="checkbox"/>	<input type="checkbox"/>	

Regularly Monitor and Test Networks

Requirement 11: Regularly test security systems and processes

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

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

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

Maintain an Information Security Policy

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

PCI DSS Question		Response:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel? <i>For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Is the information security policy reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Are usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all personnel, and require the following:				
12.3.1	Explicit approval by authorized parties to use the technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentication for use of the technology?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	A list of all such devices and personnel with access?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	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"/>	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Are the following information security management responsibilities formally assigned to an individual or team:				
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"/>	
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?		<input type="checkbox"/>	<input type="checkbox"/>	

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

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> *
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows:				
12.8.1	Is a list of service providers maintained?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possesses?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status, at least annually?		<input type="checkbox"/>	<input type="checkbox"/>	

Appendix A: (not used)

This page intentionally left blank

Appendix B: Compensating Controls

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

Compensating controls must satisfy the following criteria:

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

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

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

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

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

Appendix C: Compensating Controls Worksheet

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

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

Requirement Number and Definition:

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

Compensating Controls Worksheet—Completed Example

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

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

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

