



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

---

**Merchants with Payment Application  
Systems Connected to the Internet –  
No Electronic Cardholder Data Storage**

For use with PCI DSS Version 3.1

Revision 1.1

July 2015

## Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1</i> .
July 2015	3.1	1.1	Updated to remove references to “best practices” prior to June 30, 2015.

# Table of Contents

---

<b>Document Changes .....</b>	<b>i</b>
<b>Before You Begin.....</b>	<b>iii</b>
<b>PCI DSS Self-Assessment Completion Steps.....</b>	<b>iii</b>
<b>Understanding the Self-Assessment Questionnaire .....</b>	<b>iv</b>
<i>Expected Testing .....</i>	<i>iv</i>
<b>Completing the Self-Assessment Questionnaire.....</b>	<b>v</b>
<b>Guidance for Non-Applicability of Certain, Specific Requirements.....</b>	<b>v</b>
<b>Legal Exception .....</b>	<b>v</b>
<b>Section 1: Assessment Information .....</b>	<b>1</b>
<b>Section 2: Self-Assessment Questionnaire C.....</b>	<b>4</b>
<b>Build and Maintain a Secure Network and Systems.....</b>	<b>4</b>
<i>Requirement 1: Install and maintain a firewall configuration to protect data .....</i>	<i>4</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .....</i>	<i>6</i>
<b>Protect Cardholder Data .....</b>	<b>13</b>
<i>Requirement 3: Protect stored cardholder data .....</i>	<i>13</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks.....</i>	<i>15</i>
<b>Maintain a Vulnerability Management Program.....</b>	<b>18</b>
<i>Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs .....</i>	<i>18</i>
<i>Requirement 6: Develop and maintain secure systems and applications .....</i>	<i>20</i>
<b>Implement Strong Access Control Measures .....</b>	<b>22</b>
<i>Requirement 7: Restrict access to cardholder data by business need to know .....</i>	<i>22</i>
<i>Requirement 8: Identify and authenticate access to system components.....</i>	<i>23</i>
<i>Requirement 9: Restrict physical access to cardholder data.....</i>	<i>24</i>
<b>Regularly Monitor and Test Networks.....</b>	<b>28</b>
<i>Requirement 10: Track and monitor all access to network resources and cardholder data .....</i>	<i>28</i>
<i>Requirement 11: Regularly test security systems and processes .....</i>	<i>31</i>
<b>Maintain an Information Security Policy .....</b>	<b>36</b>
<i>Requirement 12: Maintain a policy that addresses information security for all personnel .....</i>	<i>36</i>
<b>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.....</b>	<b>40</b>
<b>Appendix B: Compensating Controls Worksheet.....</b>	<b>41</b>
<b>Appendix C: Explanation of Non-Applicability .....</b>	<b>42</b>
<b>Section 3: Validation and Attestation Details .....</b>	<b>43</b>

## Before You Begin

---

SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.).

SAQ C merchants process cardholder data via a point-of-sale (POS) system 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 mail/telephone-order (card-not-present) merchants.

SAQ C merchants confirm that, for this payment channel:

- 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 system/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);
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only;
- Your company retains only paper reports or paper copies of receipts, and these documents are not received electronically; **and**
- Your company does not store cardholder data in electronic format.

***This SAQ is not applicable to e-commerce channels.***

This shortened version of the SAQ includes questions that 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 that 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 Self-Assessment Completion Steps

1. Identify the applicable SAQ for your environment – refer to the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website for information.
2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using (as defined in Part 2g of the Attestation of Compliance).
3. Assess your environment for compliance with applicable PCI DSS requirements.
4. Complete all sections of this document:
  - Section 1 (Part 1 & 2 of the AOC) – Assessment Information and Executive Summary.
  - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ C)
  - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
5. Submit the SAQ and Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand or other requester.

## Understanding the Self-Assessment Questionnaire

The questions contained in the “PCI DSS Question” column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS <i>(PCI Data Security Standard Requirements and Security Assessment Procedures)</i>	<ul style="list-style-type: none"> <li>• Guidance on Scoping</li> <li>• Guidance on the intent of all PCI DSS Requirements</li> <li>• Details of testing procedures</li> <li>• Guidance on Compensating Controls</li> </ul>
SAQ Instructions and Guidelines documents	<ul style="list-style-type: none"> <li>• Information about all SAQs and their eligibility criteria</li> <li>• How to determine which SAQ is right for your organization</li> </ul>
<i>PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms</i>	<ul style="list-style-type: none"> <li>• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires</li> </ul>

These and other resources can be found on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

### **Expected Testing**

The instructions provided in the “Expected Testing” column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

## Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. **Only one response should be selected for each question.**

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
<b>Yes</b>	The expected testing has been performed, and all elements of the requirement have been met as stated.
<b>Yes with CCW</b> (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.  All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ.  Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
<b>No</b>	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
<b>N/A</b> (Not Applicable)	The requirement does not apply to the organization's environment. (See <i>Guidance for Non-Applicability of Certain, Specific Requirements</i> below for examples.)  All responses in this column require a supporting explanation in Appendix C of the SAQ.

## Guidance for Non-Applicability of Certain, Specific Requirements

While many organizations completing SAQ C will need to validate compliance with every PCI DSS requirement in this SAQ, 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 PCI DSS that are specific to managing wireless technology (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Note that Requirement 11.1 (use of processes to identify unauthorized wireless access points) must still be answered even if you don't use wireless technologies in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

## Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

### Part 1. Merchant and Qualified Security Assessor Information

#### Part 1a. Merchant Organization Information

Company Name:		DBA (doing business as):	
Contact Name:		Title:	
ISA Name(s) (if applicable):		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

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

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

### Part 2. Executive Summary

#### Part 2a. Type of Merchant Business (check all that apply)

<input type="checkbox"/> Retailer	<input type="checkbox"/> Telecommunication	<input type="checkbox"/> Grocery and Supermarkets
<input type="checkbox"/> Petroleum	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Mail order/telephone order (MOTO)
<input type="checkbox"/> Others (please specify):		

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
<input type="checkbox"/> Mail order/telephone order (MOTO)	<input type="checkbox"/> Mail order/telephone order (MOTO)
<input type="checkbox"/> E-Commerce	<input type="checkbox"/> E-Commerce
<input type="checkbox"/> Card-present (face-to-face)	<input type="checkbox"/> Card-present (face-to-face)

**Note:** If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.

### Part 2b. Description of Payment Card Business

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

### Part 2c. Locations

List types of facilities and a summary of locations (for example, retail outlets, corporate offices, data centers, call centers, etc.) included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>

### Part 2d. Payment Application

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

### Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes

No

**Part 2f. Third-Party Service Providers**

Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?  Yes  No

**If Yes:**

Name of service provider:	Description of services provided:

**Note:** Requirement 12.8 applies to all entities in this list.

**Part 2g. Eligibility to Complete SAQ C**

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

- Merchant has a payment application system and an Internet 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;
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only;
- Merchant does not store cardholder data in electronic format; **and**
- If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.

## Section 2: 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.

Self-assessment completion date:

### Build and Maintain a Secure Network and Systems

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:  <b>Note:</b> 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.					
1.2.1	(a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?  (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)?	<ul style="list-style-type: none"> <li>▪ Review firewall and router configuration standards</li> <li>▪ Examine firewall and router configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	<ul style="list-style-type: none"> <li>▪ Review firewall and router configuration standards</li> <li>▪ Examine firewall and router configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
1.3	Is direct public access prohibited 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?	<ul style="list-style-type: none"> <li>Examine firewall and router configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	<ul style="list-style-type: none"> <li>Examine firewall and router configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>Examine firewall and router configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network? <i>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).</i>	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Examine vendor documentation</li> <li>Observe system configurations and account settings</li> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Review vendor documentation</li> <li>Examine system configurations and account settings</li> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, 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?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Review vendor documentation</li> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are default SNMP community strings on wireless devices changed at installation?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Review vendor documentation</li> <li>Interview personnel</li> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are default passwords/passphrases on access points changed at installation?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Interview personnel</li> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Review vendor documentation</li> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(e) Are other security-related wireless vendor defaults changed, if applicable?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Review vendor documentation</li> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2	(a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?  <i>Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> <li>▪ Review system configuration standards</li> <li>▪ Review industry-accepted hardening standards</li> <li>▪ Review policies and procedures</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are system configuration standards applied when new systems are configured?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(d) Do system configuration standards include all of the following: <ul style="list-style-type: none"> <li>• Changing of all vendor-supplied defaults and elimination of unnecessary default accounts?</li> <li>• Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?</li> <li>• Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?</li> <li>• Implementing additional security features for any required services, protocols or daemons that are considered to be insecure?</li> <li>• Configuring system security parameters to prevent misuse?</li> <li>• Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review system configuration standards</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?  <i>For example, web servers, database servers, and DNS should be implemented on separate servers.</i>	<ul style="list-style-type: none"> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	<ul style="list-style-type: none"> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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)?	<ul style="list-style-type: none"> <li>▪ Review configuration standards</li> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	<ul style="list-style-type: none"> <li>Review configuration standards</li> <li>Interview personnel</li> <li>Examine configuration settings</li> <li>Compare enabled services, etc. to documented justifications</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	<p>Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?</p> <p><i>For example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.</i></p> <p><b>Note:</b> <i>SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.</i></p> <p><i>Effective immediately, new implementations must not use SSL or early TLS.</i></p> <p><i>POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</i></p>	<ul style="list-style-type: none"> <li>Review configuration standards</li> <li>Examine configuration settings</li> </ul> <p><i>If SSL/early TLS is used:</i></p> <ul style="list-style-type: none"> <li>Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS</li> </ul> <p><i>and/or</i></p> <ul style="list-style-type: none"> <li>Review Risk Mitigation and Migration Plan</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	<ul style="list-style-type: none"> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are common system security parameters settings included in the system configuration standards?	<ul style="list-style-type: none"> <li>Review system configuration standards</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(c) Are security parameter settings set appropriately on system components?	<ul style="list-style-type: none"> <li>Examine system components</li> <li>Examine security parameter settings</li> <li>Compare settings to system configuration standards</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	(a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	<ul style="list-style-type: none"> <li>Examine security parameters on system components</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are enabled functions documented and do they support secure configuration?	<ul style="list-style-type: none"> <li>Review documentation</li> <li>Examine security parameters on system components</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is only documented functionality present on system components?	<ul style="list-style-type: none"> <li>Review documentation</li> <li>Examine security parameters on system components</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3	<p>Is non-console administrative access encrypted as follows:</p> <p><i>Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.</i></p> <p><b>Note:</b> <i>SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.</i></p> <p><i>Effective immediately, new implementations must not use SSL or early TLS.</i></p> <p><i>POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</i></p>					

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
(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?	<ul style="list-style-type: none"> <li>Examine system components</li> <li>Examine system configurations</li> <li>Observe an administrator log on</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>Examine system components</li> <li>Examine services and files</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	<ul style="list-style-type: none"> <li>Examine system components</li> <li>Observe an administrator log on</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	<ul style="list-style-type: none"> <li>Examine system components</li> <li>Review vendor documentation</li> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) <i>For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:</i>  Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?	<ul style="list-style-type: none"> <li>Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p>(f) <i>For all other environments using SSL and/or early TLS:</i> Does the documented Risk Mitigation and Migration Plan include the following?</p> <ul style="list-style-type: none"> <li>• Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;</li> <li>• Risk assessment results and risk reduction controls in place;</li> <li>• Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;</li> <li>• Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;</li> <li>• Overview of migration project plan including target migration completion date no later than 30th June 2016.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review Risk Mitigation and Migration Plan</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>2.5 Are security policies and operational procedures for managing vendor defaults and other security parameters:</p> <ul style="list-style-type: none"> <li>▪ Documented</li> <li>▪ In use</li> <li>▪ Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review security policies and operational procedures</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Protect Cardholder Data

### Requirement 3: Protect stored cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
3.2	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Examine system configurations</li> <li>▪ Examine deletion processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):					
3.2.1	<p>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 after authorization?</p> <p><i>This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</i></p> <p><b>Note:</b> <i>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"> <li>• The cardholder's name,</li> <li>• Primary account number (PAN),</li> <li>• Expiration date, and</li> <li>• Service code</li> </ul> <p><i>To minimize risk, store only these data elements as needed for business.</i></p>	<ul style="list-style-type: none"> <li>▪ Examine data sources including:               <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Database schema</li> <li>• Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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 after authorization?	<ul style="list-style-type: none"> <li>▪ Examine data sources including:               <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Database schema</li> <li>• Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	<ul style="list-style-type: none"> <li>▪ Examine data sources including:               <ul style="list-style-type: none"> <li>• Incoming transaction data</li> <li>• All logs</li> <li>• History files</li> <li>• Trace files</li> <li>• Database schema</li> <li>• Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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) such that only personnel with a legitimate business need can see the full PAN?</p> <p><b>Note:</b> This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.</p>	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Review roles that need access to displays of full PAN</li> <li>▪ Examine system configurations</li> <li>▪ Observe displays of PAN</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p>4.1 (a) Are strong cryptography and security protocols, such as TLS, SSH or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?</p> <p><i>Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).</i></p> <p><b>Note:</b> SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.</p> <p><i>Effective immediately, new implementations must not use SSL or early TLS.</i></p> <p><i>POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</i></p>	<ul style="list-style-type: none"> <li>Review documented standards</li> <li>Review policies and procedures</li> <li>Review all locations where CHD is transmitted or received</li> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Are only trusted keys and/or certificates accepted?	<ul style="list-style-type: none"> <li>Observe inbound and outbound transmissions</li> <li>Examine keys and certificates</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	<ul style="list-style-type: none"> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	<ul style="list-style-type: none"> <li>Review vendor documentation</li> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p>(e) For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?</p> <p><i>For example, for browser-based implementations:</i></p> <ul style="list-style-type: none"> <li>• “HTTPS” appears as the browser Universal Record Locator (URL) protocol, and</li> <li>• Cardholder data is only requested if “HTTPS” appears as part of the URL.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(f) For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:</p> <p>Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?</p>	<ul style="list-style-type: none"> <li>▪ Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(g) For all other environments using SSL and/or early TLS: Does the documented Risk Mitigation and Migration Plan include the following?</p> <ul style="list-style-type: none"> <li>• Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;</li> <li>• Risk assessment results and risk reduction controls in place;</li> <li>• Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;</li> <li>• Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;</li> <li>• Overview of migration project plan including target migration completion date no later than 30th June 2016.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review Risk Mitigation and Migration Plan</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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? <b>Note: The use of WEP as a security control is prohibited.</b>	<ul style="list-style-type: none"> <li>▪ Review documented standards</li> <li>▪ Review wireless networks</li> <li>▪ Examine system configuration settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Maintain a Vulnerability Management Program

### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	<ul style="list-style-type: none"> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Are 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)?	<ul style="list-style-type: none"> <li>Review vendor documentation</li> <li>Examine system configurations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	<ul style="list-style-type: none"> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Are all anti-virus mechanisms maintained as follows:					
	(a) Are all anti-virus software and definitions kept current?	<ul style="list-style-type: none"> <li>Examine policies and procedures</li> <li>Examine anti-virus configurations, including the master installation</li> <li>Examine system components</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are automatic updates and periodic scans enabled and being performed?	<ul style="list-style-type: none"> <li>Examine anti-virus configurations, including the master installation</li> <li>Examine system components</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	<ul style="list-style-type: none"> <li>Examine anti-virus configurations</li> <li>Review log retention processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.3	<p>Are all anti-virus mechanisms:</p> <ul style="list-style-type: none"> <li>▪ Actively running?</li> <li>▪ Unable to be disabled or altered by users?</li> </ul> <p><b>Note:</b> <i>Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.</i></p>	<ul style="list-style-type: none"> <li>▪ Examine anti-virus configurations</li> <li>▪ Examine system components</li> <li>▪ Observe processes</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p>6.1</p> <p>Is there a process to identify security vulnerabilities, including the following:</p> <ul style="list-style-type: none"> <li>▪ Using reputable outside sources for vulnerability information?</li> <li>▪ Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities?</li> </ul> <p><b>Note:</b> Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.</p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.</p>	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Interview personnel</li> <li>▪ Observe processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are critical security patches installed within one month of release? <i>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Examine system components</li> <li>Compare list of security patches installed to recent vendor patch lists</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Implement Strong Access Control Measures

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

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:					
7.1.2	Is access to privileged user IDs restricted as follows: <ul style="list-style-type: none"> <li>▪ To least privileges necessary to perform job responsibilities?</li> <li>▪ Assigned only to roles that specifically require that privileged access?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine written access control policy</li> <li>▪ Interview personnel</li> <li>▪ Interview management</li> <li>▪ Review privileged user IDs</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Are access assigned based on individual personnel's job classification and function?	<ul style="list-style-type: none"> <li>▪ Examine written access control policy</li> <li>▪ Interview management</li> <li>▪ Review user IDs</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Requirement 8: Identify and authenticate access to system components**

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1.5	(a) Are accounts used by vendors to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	<ul style="list-style-type: none"> <li>▪ Review password procedures</li> <li>▪ Interview personnel</li> <li>▪ Observe processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are vendor remote access accounts monitored when in use?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	<p>Is two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)?</p> <p><b>Note:</b> 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.</p> <p>Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.</p>	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> <li>▪ Examine system configurations</li> <li>▪ Observe personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.1.2	<p>Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?</p> <p><i>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.</i></p>	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Interview personnel</li> <li>Observe locations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	<p>Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?</p> <p><i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i></p>	<ul style="list-style-type: none"> <li>Review policies and procedures for physically securing media</li> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	<ul style="list-style-type: none"> <li>Review policies and procedures for distribution of media</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	<ul style="list-style-type: none"> <li>Review policies and procedures for media classification</li> <li>Interview security personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	<ul style="list-style-type: none"> <li>Interview personnel</li> <li>Examine media distribution tracking logs and documentation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	<ul style="list-style-type: none"> <li>Interview personnel</li> <li>Examine media distribution tracking logs and documentation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Is strict control maintained over the storage and accessibility of media?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	<ul style="list-style-type: none"> <li>▪ Review periodic media destruction policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is media destruction performed as follows:					
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	<ul style="list-style-type: none"> <li>• Review periodic media destruction policies and procedures</li> <li>• Interview personnel</li> <li>• Observe processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	<ul style="list-style-type: none"> <li>• Examine security of storage containers</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?  <i>Note: This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.</i>					
	(a) Do policies and procedures require that a list of such devices be maintained?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	<ul style="list-style-type: none"> <li>▪ Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.9.1	(a) Does the list of devices include the following? <ul style="list-style-type: none"> <li>• Make, model of device</li> <li>• Location of device (for example, the address of the site or facility where the device is located)</li> <li>• Device serial number or other method of unique identification</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine the list of devices</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is the list accurate and up to date?	<ul style="list-style-type: none"> <li>▪ Observe devices and device locations and compare to list</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2	(a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?  <i>Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.</i>	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe inspection processes and compare to defined processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are personnel are aware of procedures for inspecting devices?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?					
	(c) Do training materials for personnel at point-of-sale locations include the following? <ul style="list-style-type: none"> <li>• Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.</li> <li>• Do not install, replace, or return devices without verification.</li> <li>• Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).</li> <li>• Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review training materials</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	<ul style="list-style-type: none"> <li>▪ Interview personnel at POS locations</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Regularly Monitor and Test Networks

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

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:					
10.2.2	All actions taken by any individual with root or administrative privileges?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Invalid logical access attempts?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Type of event?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.3	Date and time?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.3.4	Success or failure indication?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	Origination of event?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identity or name of affected data, system component, or resource?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe audit logs</li> <li>▪ Examine audit log settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows?  <b>Note:</b> Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.					
10.6.1	(b) Are the following logs and security events reviewed at least daily, either manually or via log tools? <ul style="list-style-type: none"> <li>• All security events</li> <li>• Logs of all system components that store, process, or transmit CHD and/or SAD</li> <li>• Logs of all critical system components</li> <li>• Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review security policies and procedures</li> <li>▪ Observe processes</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2	(b) Are logs of all other system components periodically reviewed—either manually or via log tools—based on the organization’s policies and risk management strategy?	<ul style="list-style-type: none"> <li>▪ Review security policies and procedures</li> <li>▪ Review risk assessment documentation</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.6.3	(b) Is follow up to exceptions and anomalies identified during the review process performed?	<ul style="list-style-type: none"> <li>▪ Review security policies and procedures</li> <li>▪ Observe processes</li> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(b) Are audit logs retained for at least one year?	<ul style="list-style-type: none"> <li>▪ Review security policies and procedures</li> <li>▪ Interview personnel</li> <li>▪ Examine audit logs</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are at least the last three months' logs immediately available for analysis?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> <li>▪ Observe processes</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
11.1 (a) Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?  <i>Note: 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. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1 (b) Does the methodology detect and identify any unauthorized wireless access points, including at least the following? <ul style="list-style-type: none"> <li>WLAN cards inserted into system components;</li> <li>Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and</li> <li>Wireless devices attached to a network port or network device.</li> </ul>	<ul style="list-style-type: none"> <li>Evaluate the methodology</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1 (c) If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?	<ul style="list-style-type: none"> <li>Examine output from recent wireless scans</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1 (d) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?	<ul style="list-style-type: none"> <li>Examine configuration settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.1 Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?	<ul style="list-style-type: none"> <li>Examine inventory records</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.1.2	(a) Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?	<ul style="list-style-type: none"> <li>Examine incident response plan (see Requirement 12.10)</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is action taken when unauthorized wireless access points are found?	<ul style="list-style-type: none"> <li>Interview responsible personnel</li> <li>Inspect recent wireless scans and related responses</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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><b>Note:</b> Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.</p> <p>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 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(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</p>					

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.2.1	(a) Are quarterly internal vulnerability scans performed?	<ul style="list-style-type: none"> <li>Review scan reports</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Does the quarterly internal scan process include rescans as needed until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	<ul style="list-style-type: none"> <li>Review scan reports</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are quarterly internal 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)?	<ul style="list-style-type: none"> <li>Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2	(a) Are quarterly external vulnerability scans performed? <i>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.</i>	<ul style="list-style-type: none"> <li>Review results from the four most recent quarters of external vulnerability scans</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	<ul style="list-style-type: none"> <li>Review results of each external quarterly scan and rescan</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?	<ul style="list-style-type: none"> <li>Review results of each external quarterly scan and rescan</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
11.2.3 (a) Are internal and external scans, and rescans as needed, performed after any significant change? <b>Note: Scans must be performed by qualified personnel.</b>	<ul style="list-style-type: none"> <li>▪ Examine and correlate change control documentation and scan reports</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Does the scan process include rescans until: <ul style="list-style-type: none"> <li>• For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS,</li> <li>• For internal scans, a passing result is obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review scan reports</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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)?	<ul style="list-style-type: none"> <li>▪ Interview personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4 If segmentation is used to isolate the CDE from other networks:					
(a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?	<ul style="list-style-type: none"> <li>▪ Examine segmentation controls</li> <li>▪ Review penetration-testing methodology</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Does penetration testing to verify segmentation controls meet the following? <ul style="list-style-type: none"> <li>• Performed at least annually and after any changes to segmentation controls/methods</li> <li>• Covers all segmentation controls/methods in use</li> <li>• Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine results from the most recent penetration test</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.5	<p>(a) Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?</p> <p><i>Examples of files that should be monitored include:</i></p> <ul style="list-style-type: none"> <li>• System executables</li> <li>• Application executables</li> <li>• Configuration and parameter files</li> <li>• Centrally stored, historical or archived, log, and audit files</li> <li>• Additional critical files determined by entity (for example, through risk assessment or other means)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Observe system settings and monitored files</li> <li>▪ Examine system configuration settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<p>(b) Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly?</p> <p><b>Note:</b> For change detection 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. Change detection mechanisms such as 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).</p>	<ul style="list-style-type: none"> <li>▪ Observe system settings and monitored files</li> <li>▪ Review results from monitoring activities</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	<ul style="list-style-type: none"> <li>▪ Examine system configuration settings</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Maintain an Information Security Policy

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

**Note:** 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.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	<ul style="list-style-type: none"> <li>Review the information security policy</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	<ul style="list-style-type: none"> <li>Review the information security policy</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following: <b>Note:</b> Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.					
12.3.1	Explicit approval by authorized parties to use the technologies?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Authentication for use of the technology?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	A list of all such devices and personnel with access?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Acceptable uses of the technologies?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Acceptable network locations for the technologies?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>Review usage policies</li> <li>Interview responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	<ul style="list-style-type: none"> <li>Review information security policy and procedures</li> <li>Interview a sample of responsible personnel</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5	(b) 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?	<ul style="list-style-type: none"> <li>Review information security policy and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>Review security awareness program</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
12.8.1	Is a list of service providers maintained?	<ul style="list-style-type: none"> <li>Review policies and procedures</li> <li>Observe processes</li> <li>Review list of service providers</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.2	<p>Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?</p> <p><b>Note:</b> The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</p>	<ul style="list-style-type: none"> <li>Observe written agreements</li> <li>Review policies and procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<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?	<ul style="list-style-type: none"> <li>Observe processes</li> <li>Review policies and procedures and supporting documentation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	<ul style="list-style-type: none"> <li>Observe processes</li> <li>Review policies and procedures and supporting documentation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	<ul style="list-style-type: none"> <li>Observe processes</li> <li>Review policies and procedures and supporting documentation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?	<ul style="list-style-type: none"> <li>▪ Review the incident response plan</li> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Does the plan address the following, at a minimum:					
<ul style="list-style-type: none"> <li>• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Specific incident response procedures?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Business recovery and continuity procedures?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Data backup processes?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Analysis of legal requirements for reporting compromises?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Coverage and responses of all critical system components?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Reference or inclusion of incident response procedures from the payment brands?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review incident response plan procedures</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## **Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers**

This appendix is not used for merchant assessments.

## Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where “YES with CCW” was checked.

**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.

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

### Requirement Number and Definition:

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



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

Based on the results noted in the SAQ C dated (*completion date*), the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of (*date*): (**check one**):

- Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; 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 affirmatively, resulting in an overall **NON-COMPLIANT** rating, 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.*
- Compliant but with Legal exception:** One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.  
*If checked, complete the following:*
- | Affected Requirement | Details of how legal constraint prevents requirement being met |
|----------------------|--|
|                      |  |
|                      |  |

### Part 3a. Acknowledgement of Status

**Signatory(s) confirms:**  
*(Check all that apply)*

- PCI DSS Self-Assessment Questionnaire C, 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 PCI DSS compliance, as applicable to my environment, at all times.
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

- No evidence of full track data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor (*ASV Name*)

**Part 3b. Merchant Attestation**

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

**Part 3c. QSA Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:	
--	--

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i>
<i>Duly Authorized Officer Name:</i>	<i>QSA Company:</i>

**Part 3d. ISA Acknowledgement (if applicable)**

If a ISA was involved or assisted with this assessment, describe the role performed:	
--	--

<i>Signature of ISA</i> ↑	<i>Date:</i>
<i>ISA Name:</i>	<i>Title:</i>

<sup>1</sup> 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 track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to 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.*

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		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	Protect all systems against malware 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	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	

\* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

