Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire P2PE and Attestation of Compliance

---

Merchants using Hardware Payment Terminals in a PCI SSC-Listed P2PE Solution Only – 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
N/A	1.0		Not used.
May 2012	2.0		To create SAQ P2PE-HW for merchants using only hardware terminals as part of a validated P2PE solution listed by PCI SSC. This SAQ is for use with PCI DSS v2.0.
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 *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1*. Removed "HW" from SAQ title, as may be used by merchants using either a HW/HW or HW/Hybrid P2PE solution.
July 2015	3.1	1.1	Updated to remove references to "best practices" prior to June 30, 2015.

Table of Contents

Before you Begin

Merchant Eligibility Criteria for SAQ P2PE

SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a validated P2PE hardware device.

SAQ P2PE merchants confirm that, for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC;
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution;
- Your company does not otherwise receive or transmit cardholder data electronically.
- There is no legacy storage of electronic cardholder data in the environment;
- If your company stores cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically, **and**
- Your company has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.

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.

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. Confirm that you have implemented all elements of the PIM.
4. Assess your environment for compliance with the applicable PCI DSS requirements.
5. 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 P2PE)
    - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details, and Action Plan for Non-Compliant Requirements (if applicable)
6. Submit the SAQ and the Attestation of Compliance—along with any other requested documentation—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 *(PCI Data Security Standard Requirements and Security Assessment Procedures)*	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website *(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:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (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.
No	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.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. (See Guidance for Non-Applicability of Certain, Specific Requirements 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

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 (PCI DSS) Requirements and Security Assessment Procedures*. Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your 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:		ZIP:	
URL:					

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

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

Part 2. Executive Summary

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

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

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Card-present (face-to-face)	☐ 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 (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

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

Part 2d. P2PE Solution

Provide the following information regarding the validated PCI P2PE solution your organization uses:

Name of P2PE Solution Provider:	
Name of P2PE Solution:	
PCI SSC Reference Number	
Listed P2PE POI Devices used by Merchant (PTS Device Dependencies):	

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, airline booking agents, loyalty program agents, etc.)? ***If Yes:***	☐ Yes ☐ No

Name of service provider:	Description of services provided:

Note: *Requirement 12.8 applies to all entities listed in response to this question.*

Part 2g. Eligibility to Complete SAQ P2PE	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	All payment processing is via the validated PCI P2PE solution approved and listed by the PCI SSC (per above).
☐	The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution.
☐	Merchant does not otherwise receive or transmit cardholder data electronically.
☐	Merchant verifies there is no legacy storage of electronic cardholder data in the environment.
☐	If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically, **and**
☐	Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

Section 2: Self-Assessment Questionnaire P2PE

Note: *The following questions are numbered according to the actual PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document. As only a subset of PCI DSS requirements are provided in this SAQ P2PE, the numbering of these questions may not be consecutive.*

Self-assessment completion date:

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Note: *Requirement 3 applies only to SAQ P2PE merchants that have paper records (for example, receipts, printed reports, etc.) with account data, including primary account numbers (PANs).*

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
3.1	Are data-retention and disposal policies, procedures, and processes implemented as follows:					
	(a) Is data storage amount and retention time limited to that required for legal, regulatory, and/or business requirements?	▪ Review data retention and disposal policies and procedures ▪ Interview personnel	☐	☐	☐	☐
	(b) Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, and/or business reasons?	▪ Review policies and procedures ▪ Interview personnel ▪ Examine deletion mechanism	☐	☐	☐	☐
	(c) Are there specific retention requirements for cardholder data? *For example, cardholder data needs to be held for X period for Y business reasons.*	▪ Review policies and procedures ▪ Interview personnel ▪ Examine retention requirements	☐	☐	☐	☐
	(d) Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?	▪ Review policies and procedures ▪ Interview personnel ▪ Observe deletion processes	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(e) Does all stored cardholder data meet the requirements defined in the data-retention policy?	▪ Examine files and system records	☐	☐	☐	☐
Guidance: *"Yes" answers for requirements at 3.1 mean that if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed.* *If a merchant never prints or stores any paper containing account data, the merchant should mark the "N/A" column and complete the "Explanation of Non-Applicability" worksheet in Appendix C.*						
3.2.2	For all paper storage, 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?	▪ Examine paper data sources	☐	☐	☐	☐
Guidance: *A "Yes" answer for Requirement 3.2.2 means that if the merchant writes down the card security code while a transaction is being conducted, the merchant either securely destroys the paper (for example, with a shredder) immediately after the transaction is complete, or obscures the code (for example, by "blacking it out" with a marker) before the paper is stored.* *If the merchant never requests the three-digit or four-digit number printed on the front or back of a payment card ("card security code"), the merchant should mark the "N/A" column and complete the "Explanation of Non-Applicability" worksheet in Appendix C.*						
3.3	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 as follows? ***Note:*** *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.*	▪ Review policies and procedures ▪ Review roles that need access to displays of full PAN ▪ Examine system configurations ▪ Observe displays of PAN	☐	☐	☐	☐
Guidance: *A "Yes" answer to Requirement 3.3 means that any PANs displayed on paper show at most only the first six and last four digits.* *If the merchant never displays or prints PAN on paper, the merchant should mark the "N/A" column and complete the "Explanation of Non-Applicability" worksheet in Appendix C.*						

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
3.7	Are security policies and operational procedures for protecting stored cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐
Guidance: *A "Yes" answer to Requirement 3.7 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place for Requirements 3.1, 3.2.2, and 3.3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.*						

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
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	▪ Review policies and procedures	☐	☐	☐	☐
Guidance: *A "Yes" answer to Requirement 4.2 means that the merchant has a written document or policy for employees, so they know they cannot use e-mail, instant messaging or chat (or other end-user messaging technologies) to send PANs, for example, to other employees or to customers.*						

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

Note: *Requirements 9.5 and 9.8 apply only to SAQ P2PE merchants that have paper records (for example, receipts, printed reports, etc.) with account data, including primary account numbers (PANs).*

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	▪ Review policies and procedures for physically securing media ▪ Interview personnel	☐	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	▪ Review periodic media destruction policies and procedures	☐	☐	☐	☐
	(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?	▪ Review periodic media destruction policies and procedures ▪ Interview personnel ▪ Observe processes	☐	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	▪ Review periodic media destruction policies and procedures ▪ Examine security of storage containers	☐	☐	☐	☐

Guidance: *"Yes" answers for requirements at 9.5 and 9.8 mean that the merchant securely stores any paper with account data, for example by storing them in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees so they know how to secure paper with account data and how to destroy the paper when no longer needed.*

If the merchant never stores any paper with account data, the merchant should mark the "N/A" column and complete the "Explanation of Non-Applicability" worksheet in Appendix C.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.9	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? ***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.*					
	(a) Do policies and procedures require that a list of such devices be maintained?	▪ Review policies and procedures	☐	☐	☐	☐
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	▪ Review policies and procedures	☐	☐	☐	☐
	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	▪ Review policies and procedures	☐	☐	☐	☐
9.9.1	(a) Does the list of devices include the following? • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	▪ Examine the list of devices	☐	☐	☐	☐
	(b) Is the list accurate and up to date?	▪ Observe devices and device locations and compare to list	☐	☐	☐	☐
	(c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	▪ Interview personnel	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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? ***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.*	▪ Interview personnel ▪ Observe inspection processes and compare to defined processes	☐	☐	☐	☐
	(b) Are personnel are aware of procedures for inspecting devices?	▪ Interview personnel	☐	☐	☐	☐
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?					
	(a) Do training materials for personnel at point-of-sale locations include the following? • 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. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	▪ Review training materials	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(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?	▪ Interview personnel at POS locations	☐	☐	☐	☐
Guidance: *"Yes" answers to requirements at 9.9 mean the merchant has policies and procedures in place for Requirements 9.9.1 – 9.9.3, and that they maintain a current list of devices, conduct periodic device inspections, and train employees about what to look for to detect tampered or replaced devices.*						
9.10	Are security policies and operational procedures for restricting physical access to cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Examine security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐
Guidance: *A "Yes" answer to Requirement 9.10 means that the merchant has policies and procedures in place for Requirements 9.5, 9.8, and 9.9, as applicable for your environment. This helps to ensure personnel are aware of and following security policies and documented operational procedures.*						

Maintain an Information Security Policy

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

Note: Requirement 12 specifies that merchants must have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel so they are aware of their responsibilities for protecting the, payment terminals, any paper documents with cardholder data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).

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?	▪ Review the information security policy	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	▪ Review the information security policy ▪ Interview responsible personnel	☐	☐	☐	☐
Guidance: *"Yes" answers for requirements at 12.1 mean that the merchant has a security policy that is reasonable for the size and complexity of the merchant's operations, and that the policy is reviewed annually and updated if needed. For example, such a policy could be a simple document that covers how to protect the store and payment devices in accordance with* the P2PE Instruction Manual (PIM), *and who to call in an emergency.*						
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	▪ Review information security policy and procedures ▪ Interview a sample of responsible personnel	☐	☐	☐	☐
Guidance: *A "Yes" answer for Requirement 12.4 means that the merchant's security policy defines basic security responsibilities for all personnel, consistent with the size and complexity of the merchant's operations. For example, security responsibilities could be defined according to basic responsibilities by employee levels, such as the responsibilities expected of a manager/owner and those expected of clerks.*						
12.5	Are the following information security management responsibilities formally assigned to an individual or team:					
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	▪ Review information security policy and procedures	☐	☐	☐	☐
Guidance: *A "Yes" answer for Requirement 12.5.3 means that the merchant has a person designated as responsible for the incident-response and escalation plan required at 12.9.*						

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	▪ Review security awareness program	☐	☐	☐	☐
Guidance: *A Yes" answer for Requirement 12.6 means that the merchant has a security awareness program in place, consistent with the size and complexity of the merchant's operations. For example, a simple awareness program could be a flyer posted in the back office, or a periodic e-mail sent to all employees. Examples of awareness program messaging include descriptions of security tips all employees should follow, such as how to lock doors and storage containers, how to determine whether a payment terminal has been tampered with, and how to identify legitimate personnel who may come to service hardware payment terminals.*						
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?	▪ Review policies and procedures ▪ Observe processes ▪ Review list of service providers	☐	☐	☐	☐
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess 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? ***Note:*** *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.*	▪ Observe written agreements ▪ Review policies and procedures	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☐
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☐
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☐
Guidance: *"Yes" answers for requirements at 12.8 mean that the merchant has a list of, and agreements with, service providers they share cardholder data with. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data.*						
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	▪ Review the incident response plan ▪ Review incident response plan procedures	☐	☐	☐	☐
Guidance: *"Yes" answers for requirements at 12.10 mean that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hotsite" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency.*						

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

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
12.8	Cardholder data is never shared with service providers.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ P2PE 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 P2PE are complete, and 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 P2PE 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, since not all payment brands require this section.*
☐	**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 P2PE, 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.
☐	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

Part 3a. Acknowledgement of Status (continued)	
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
☐	No evidence of, full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3]) was found on ANY system reviewed during this assessment.

Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↗	*Date:*
Merchant Executive Officer Name:	*Title:*

Part 3c. QSA Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↗	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. ISA Acknowledgement (if applicable)	
If a ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA ↗	*Date:*
ISA Name:	*Title:*

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

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

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

Part 4. Action Plan for Non-Compliant Status

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, since not all payment brands require this section.

PCI DSS Requirement*	Description of Requirement	Compliance to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	

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