Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire B and Attestation of Compliance

Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals – No Electronic Cardholder Data Storage

For use with PCI DSS Version 3.2

Revision 1.1
January 2017

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 *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1*.
July 2015	3.1	1.1	Updated to remove references to "best practices" prior to June 30, 2015.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.*
January 2017	3.2	1.1	Updated version numbering to align with other SAQs

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Table of Contents

Document Changes ..... **i**

Before You Begin ..... **iii**

PCI DSS Self-Assessment Completion Steps ..... **iii**

Understanding the Self-Assessment Questionnaire ..... **iv**

Expected Testing ..... *iv*

Completing the Self-Assessment Questionnaire ..... **v**

Guidance for Non-Applicability of Certain, Specific Requirements ..... **v**

Legal Exception ..... **v**

Section 1: Assessment Information **1**

Section 2: Self-Assessment Questionnaire B **4**

Protect Cardholder Data **4**

Requirement 3: Protect stored cardholder data *4*

Requirement 4: Encrypt transmission of cardholder data across open, public networks *6*

Implement Strong Access Control Measures **7**

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

Requirement 9: Restrict physical access to cardholder data *8*

Maintain an Information Security Policy **12**

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

Appendix A: Additional PCI DSS Requirements **15**

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers *15*

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS *15*

Appendix A3: Designated Entities Supplemental Validation (DESV) *15*

Appendix B: Compensating Controls Worksheet **16**

Appendix C: Explanation of Non-Applicability **17**

Section 3: Validation and Attestation Details **18**

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Before You Begin

SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B merchants confirm that, for this payment channel:

- Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- Your company does not transmit cardholder data over a network (either an internal network or the Internet);
- Any cardholder data your company retains is on paper (for example, printed reports or 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 (Parts 1 & 2 of the AOC) – Assessment Information and Executive Summary.
   - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ B)
   - 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 (AOC), along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand or other requester.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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:		
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	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ 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.*

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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)
Example: Retail outlets	*3*	*Boston, MA, USA*

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)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2f. Third-Party Service Providers	
Does your company use a Qualified Integrator & Reseller (QIR)? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☐ No
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), 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 B	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data over either a phone line or the Internet; and/or Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
☐	Merchant does not transmit cardholder data over a network (either an internal network or the Internet);
☐	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.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Self-Assessment Questionnaire B

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:

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?	▪ Review policies and procedures ▪ Examine system configurations ▪ Examine deletion processes	☐	☐	☐	☐
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):					
3.2.1	The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization? *This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.* ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name,* • *Primary account number (PAN),* • *Expiration date, and* • *Service code* *To minimize risk, store only these data elements as needed for business.*	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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?	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☐
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☐
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 more than the first six/last four digits of the PAN? ***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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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: ▪ To least privileges necessary to perform job responsibilities? ▪ Assigned only to roles that specifically require that privileged access?	▪ Examine written access control policy ▪ Interview personnel ▪ Interview management ▪ Review privileged user IDs	☐	☐	☐	☐
7.1.3	Is access assigned based on individual personnel's job classification and function?	▪ Examine written access control policy ▪ Interview management ▪ Review user IDs	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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
9.5	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	☐	☐	☐	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	▪ Review policies and procedures for distribution of media	☐	☐	☐	☐
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	▪ Review policies and procedures for media classification ▪ Interview security personnel	☐	☐	☐	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☐
9.7	Is strict control maintained over the storage and accessibility of media?	▪ Review policies and procedures	☐	☐	☐	☐
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(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	☐	☐	☐	☐
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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 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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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?	▪ 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	☐	☐	☐	☐
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following: ***Note:*** *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?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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?	▪ Review information security policy and procedures	☐	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	▪ Review security awareness program	☐	☐	☐	☐
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, including a description of the service(s) provided?	▪ 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	☐	☐	☐	☐
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	☐	☐	☐	☐
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	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

This appendix is not used for SAQ B merchant assessments

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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.	

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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:	
3.4	Cardholder data is never stored electronically

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ B (Section 2), dated *(SAQ completion date).*

Based on the results documented in the SAQ B noted above, 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: (***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 B, 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.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Acknowledgement of Status (continued)	
☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] 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

Signature of Merchant Executive Officer ↗	*Date:*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (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. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[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 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.

[2] 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.

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

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
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.*

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.